IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 7, 2021, accepted March 29, 2021, date of publication April 5, 2021, date of current version April 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3070841

Traffic Analysis Through Spatial and Temporal Correlation: Threat and Countermeasure

YOUSEF EBRAHIMI AND MOHAMED YOUNIS, (Senior Member, IEEE)
Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD 21250, USA
Corresponding author: Yousef Ebrahimi (yousef2@umbc.edu)

ABSTRACT The base station (BS) in a Wireless Sensor Network (WSN) plays the role of a data sink, a point of contact with the upper hierarchy, and an in-situ command and control unit. Such an essential role makes the BS a target for attacks in a hostile environment. Even if its presence is camouflaged, an adversary may locate the BS by applying traffic analysis. Basically, the adversary can intercept radio transmissions and correlate them using techniques like Evidence theory (ET). The ET attack model only uses spatial aspects of intercepted transmissions in order to deduce knowledge about data routes. In this paper, we propose an enhanced version of ET (EET) which utilizes temporal correlation of transmissions to draw further valuable insight about the network topology. Analyzing ET and extending its capability are very fundamental for the network in order to avoid the illusive sense of security by guarding against a weaker attack model than what could be potentially launched. Moreover, we develop a novel and effective countermeasure, called Assisted Deception (AD) that needs no involvement of BS and is resilient to both ET and EET. By implementing AD, nodes coordinate and inject timed deceptive packets to target temporal correlation of consecutive transmissions that EET relies on. The attack and countermeasure are validated through extensive simulation experiments.

INDEX TERMS Anonymity, evidence theory, location privacy, traffic analysis, wireless sensor networks.

I. INTRODUCTION

Miniaturized sensing and portable electronic devices have benefited greatly from the recent improvements of processing, storage, sensing, and communication technologies. Drop in production cost has made it viable to have a large deployment of sensing-enabled interconnected devices that constitute a WSN [1]. WSN is ideal for applications operating in remote and hostile environments, such as border protection, security surveillance, fire detection, combat field reconnaissance, target tracking, etc. [2], [3]. Typically, a WSN can involve a large number of nodes where they report their data to an in-situ BS via wireless links. The BS acts as the data processing unit, and interfaces the WSN network to remote users, e.g., command and control centers. The operation can be either event-driven where only specific measurements warrants reporting, e.g., when detecting a target, or time-driven where data are collected and disseminated periodically. The employed nodes are battery-operated with limited capacities. To prolong their lifespan, low-power electronics are usually used in the node design. Since communication activities are the main consumer of node's energy, multi-hop communication is the preferred method for disseminating data to the BS [2]. Since all data paths end at the BS, such a multi-hop routing topology could reveal where the BS is located and expose it to attacks. In fact, the important role that the BS plays, makes it a valuable target for intentional attacks by an adversary. Consider for example a border protection application where a WSN is employed to detect infiltration attempts. An intruder would be eager to locate the BS and launch a radio jamming attack since it is very hard to evade all deployed sensors. To protect the BS, its role, identity, and more importantly its location need to be concealed [4]. Although packet encryption and anonymous routing are often employed to safeguard against information leakage through packet sniffing [5]–[7], a capable adversary can track radio transmissions and apply traffic analysis techniques [8]–[10] to gain knowledge about whereabouts of the BS.

A. TRAFFIC ANALYSIS MODELS

Anonymity is defined as the state of being not identifiable, which is generally a qualitative metric [11]. However, a number of quantitative measures are proposed in the literature to evaluate the network's resiliency to traffic analysis attack.

The associate editor coordinating the review of this manuscript and approving it for publication was Mahdi Zareei.

Analogous to anonymity is the uncertainty of the pick from a pool of choices, which makes the probabilistic models, e.g. Evidence Theory (ET), a suitable anonymity metric. In [12], D. Huang uses the number of captured packets to quantify the evidence and build their ET model. Each packet transmission is considered as an evidence of a link between the source and its immediate receivers. Following the rule of inference, new links are derived from the collected evidence. Furthermore, a probability density (*Belief*) function is applied to all packet delivery paths. *Belief* peaks correspond to regions with high fidelity in the presence of the BS. In general, ET relies on spatial correlation of packet transmissions to form the links between a source and a destination, and is used widely in the literature as a traffic analysis attack model [8], [13]–[24]. This paper presents a new model, called Enhanced Evidence Theory (EET) that correlates the intercepted transmissions both spatially and temporally. EET factors the temporal relations between two by elevating the corresponding spatially inferred evidence through the addition of a bonus value. The added time-based correlation feature increases the accuracy of the *Belief* function in converging to the location of BS. The effectiveness of EET relies on selection of bonus value and the temporal correlation window within which two transmissions are deemed to be related. We provide guidelines on how to set these two parameters.

B. SHORTCOMINGS OF EXISTING COUNTERMEASURES

Since current countermeasures are designed with only ET in mind, they do not have any strategy in safeguarding against the temporal correlation of EET. Furthermore, many of countermeasures assume a time-driven operation model to pre-calculate the transmission load of each node and structure their defense strategy, e.g., by utilizing load balancing trees [18], [21], or rate matching [25]. However, such an assumption makes the countermeasures less effective or inapplicable for event-driven networks. In addition, centralized countermeasures like [18], [20]–[22], [26] demand continued engagement of the BS to reevaluate the level of anonymity and adapt the defense mechanisms; such BS engagement constitutes a threat since it could result in revealing the location of the BS. Furthermore, defense techniques like [17]–[23] are designed to be applicable on the grid-based mapping of the deployment area and introduce fake packet traffic based on analysis at cell-level of the grid. Such a strategy does not consider the exposed overhead on individual nodes within the cells. Thus, a cell with fewer nodes could suffer relatively high per-node overhead, causing the nodes to exhaust their energy faster and consequently the network may get partitioned. To address the aforementioned shortcomings, this paper proposes an Assisted Deception (AD) mechanism in which neighboring nodes inject coordinated deceptive packets to prevent temporal correlation of data packets. AD is distributed, dynamic, node-level (rather than cell level), EET resilient, and applicable to both time and event driven modes of WSN operation. The effectiveness of AD is demonstrated via extensive simulation experiments and is shown to surpass contemporary schemes in the literature.

C. CONTRIBUTIONS AND ORGANIZATION

A preliminary study of the potential of temporal correlation on the effectiveness of ET has been presented in [27]. This paper extends the scope by studying the impact and fine-tuning of the EET parameters, namely the bonus and time correlation window. In addition, a novel approach is proposed to dynamically set the bonus value in order to make EET adaptive to the various network topologies. In [27], a Delaying Packets Relaying (DPR) is presented. DPR is a passive approach that adds controlled delays in forwarding packets on the routing paths in order to degrade the adversary's ability in relating in and out traffic of the individual nodes. Unlike DPR, AD proposed in this paper, is an active approach that enables cooperation among the nodes and is thus more adaptive in countering adversary's attacks. AD is shown to outperform recently published schemes. The contribution can be summarized as follows:

- Develop a novel traffic analysis attack model that factors both spatial and temporal relations between the intercepted transmissions in order to locate the BS of a WSN network.
- Study the effect of the correlation parameters on the success of the traffic analysis attack and provide guidelines for appropriate settings.
- Develop an effective attack countermeasure that enables the nodes to cooperatively confuse the adversary and diminishes the probability of locating the BS.
- Analyze the accuracy of BS localization through traffic analysis and introduce new metrics to better assess the anonymity of the BS.
- Validate the performance of both the new attack and countermeasure through extensive simulation.

The rest of the paper is organized as follows. Section II discusses the considered system and threat models. Section III sets the contribution apart from related work in the literature. Section IV explains ET and highlights its shortcomings; expert readers can skip such a section. The proposed EET model is presented in Section V. The proposed AD countermeasure is described in Section VI. New anonymity metrics and simulation results are presented in Section VI. Finally, the paper is concluded in Section VII.

II. SYSTEM AND THREAT MODEL

A. NETWORK MODEL

We are considering applications of WSN in unattended setups, where stationary nodes are randomly deployed across an area of interest. These nodes have similar capabilities in terms of communication range, computational resources, and initial power. The network includes a more capable unit that serves as an in-situ BS. After initial discovery and routing setup, nodes transmit their data over multi-hop paths to the BS for local analysis and/or long-haul transmission to an offsite center. The multi-hop routing achieves node energy

conservation by minimizing the sum of the distance squared between a node and gateway, and allows for frequency reuse [28]. The BS also may be involved in coordinating the operation of the network. A relay denotes a node that serves on multi-hop paths from a source to the BS. A node generates data either periodically or based on an external trigger. For example, a node could be incorporated with sensing elements that generates data when its receptors pick up the presence of a target or detect a certain phenomenon within its field of view. While an event is present, sensors generate data samples periodically and transmit each sample in a distinct packet towards the BS.

All packets are of equal priority and first-in, first-out (FIFO) queues are used in all nodes. It is assumed that no data compression or aggregation is being used; In other words, a node forwards an incoming packet to its next hop without altering or combining it with other packets. This is customary for event-triggered data traffic since the situation evolves rather quickly and all raw data is needed for spatiotemporal analysis. The network can employ any routing algorithm of choice; nonetheless in the presentation we assume that a shortest path algorithm is employed. All nodes including the BS are assumed to be physically camouflaged to make them visually unidentifiable within the environment. Furthermore, all nodes including the BS are aware of their positions within the area by either using onboard GPS or applying geolocation techniques [29], [30]. To prevent path tracing through packet sniffing and header analysis, all traffic in the network is encrypted using pairwise keys. Packet headers, including IPs and MAC addresses, are also encrypted in the same fashion [7], [31].

B. ADVERSARY MODEL

In a hostile environment, a potential adversary will aim to be as passive as possible to prevent detection by the network. A passive global adversary is assumed in this paper, in which multiple antennas/agents are deployed to intercept all node transmissions by at least 3 antennas. The main goal of the adversary would be to inflict the most damage on the network functionality. Considering the network model presented above and the major role that the BS plays, an adversary would rather target the BS. Locating and isolating, or even destroying the BS would render the WSN useless. The adversary is assumed to have enough resources to intercept all transmissions across the deployment area, e.g., using sensitive antennas. Upon intercepting a transmission, the adversary undertakes triangulation techniques to locate the transmitter [30], [32], [33]. Fig. 1 shows an example of such techniques; Angle of Arrival (AOA). By encrypting packet headers in the network, the adversary is left with link-layer based traffic analysis, particularly observing the spatial distribution of the traffic density to gain knowledge about the network topology and the BS location. ET as a well-known and capable method for traffic analysis is assumed to be used by adversaries [12]. ET is discussed in detail in Section IV, and followed by our extended attack model in Section V.

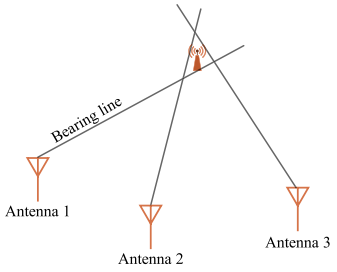

FIGURE 1. AOA, an example of triangulation technique that the adversary may use. In presence of noise/error, bearing lines do not interact at the same point.

III. RELATED WORKS

A. TAXONOMY OF TRAFFIC ANALYSIS COUNTERMEASURES

In WSN, the identity, role, and the location of the nodes could be of the interest to an adversary in order to gain knowledge about the operation of the network and/or launch an attack to interfere with it [34], [35]. Hence, the security and privacy in WSN has been a prime topic of research in recent years [4], [36]–[38]. From an adversary point of view, both the data source and sink are targets [4], [8], [39], [40]. Preventing the adversary from knowing the location of nodes that generate the data, is often referred to as source anonymity. In source anonymity studies, it is typically assumed that the adversary knows the location of the Sink/BS and traces the traffic from the vicinity of the sink node back to the source [40]–[45]. In fact, if the adversary can locate the BS, targeting it would be a more effective attack strategy. Thus, concealing the BS location is even beneficial for sustaining the anonymity of the data sources. To that endeavor, the first line of defense is to prevent extraction of any actionable information from a packet capture attack. Packet header encryption and anonymous routing strive to achieve that [6], [7], [31], [46].

With no access to the packet content, the adversary utilizes more advanced techniques such as traffic analysis that rely on intercepting and correlating radio transmissions to infer the data routes and identify the sink of the packet traffic [9], [10], [47]. Such correlation factors in attributes like the location of source node, range, rate of transmission, the potential location of destination, the time of transmission, etc. To conduct the analysis, information theoretic models have been pursued [12], [48], [49]; yet they tend to be useful in assessing anonymity rather than conducting an attack. Meanwhile, the GSAT model, proposed by Deng *et al.* [15], is used to monitor the transmission rate of nodes in order to locate the BS based on the fact that nodes closer to the BS tend to have a higher transmission rate. However, relying on traffic volume does not suffice, and additional means is needed to verify/identify the BS, e.g. visual inspection. On the other hand, the evidence theory model [12] correlates transmissions to deduce relationships among nodes. Hence, ET is deemed to be the most effective model for passive traffic

analysis and has been widely used [8], [14], [17], [19], [23]. A number of countermeasures has been proposed to boost the BS anonymity against ET model, and can be categorized as follows:

1) BS REPLICATION/RELOCATION

A popular strategy for increasing the BS anonymity is to introduce another entity that could be targeted with attack. Such strategy is often realized by mimicking the presence of: (i) a dummy BS, (ii) multiple BS, or (iii) a moving BS. In [50] the decoy sink protocol creates a dummy BS away from the real BS. All data is first forwarded to the dummy BS and then re-routed to the real BS. Wright et al. [51] goes further to propose the creation of multiple dummy sinks that are spread evenly throughout the network. Meanwhile, the focus of [52] is on multi-BS setup where the traffic is distributed to avoid making any of the BS stand out. Liu et al. [53] propose having a mobile sink to move in a semi-random circular pattern to collect the data from selected nodes that are storing the data until the BS becomes within reach. Kumar et al. in [54] divide the network into multi-layer rings. A mobile BS sends its new location to the nodes in the central ring. All nodes are preconfigured to query the central ring for the current BS position. The flow generated with such traffic creates hotspot regions within the network and distracts the adversary from the actual location of the BS. In [23], the BS mobility is exploited on demand, where the anonymity is continually assessed and the position of the BS is changed when anonymity drops below a threshold. Clearly, BS mobility and replication may be infeasible in many WSN applications.

2) INTRODUCING FAKE SINKS

When the BS cannot move or be replicated, some work has tried to introduce fake sinks that attract the adversary's attention or at least make the analysis inconclusive. The selection of fake sinks can be random [55], [56], or optimized [21], [25]. While MoRF [21] selects the fake sinks based on the topological distance to the BS and among them, IATA [25] factors in the physical proximity to the BS. Both approaches generate bogus packets and route them to the fake sinks at a rate that balances the traffic density in the network. MSI [20] extends MoRF by controlling the deceptive packet generation rates in order to turn the vicinity of fake sinks into hotspots. On the other hand, the approach of [57] strives to mimic the behavior of the BS during in-network data aggregation. Aggregator nodes (ANs) are tasked to collect the real data packets and forward them randomly to the BS via other ANs. In addition, all nodes introduce deceptive packets and the BS updates routing topology at will. CPSLP [55] uses a combination of multiple sinks, a cloud of fake source nodes, and fake packets to hide the real source from an in-situ adversary. CPSLP randomly selects a sink destination for each data packet generated. It also uses randomly selected intermediate nodes to construct its routing path from source to selected sink to further randomize the path. To boost the privacy of the source, CPSLP also creates a fake cloud and fake traffic in close proximity of the source to make it difficult for the attacker to identify the actual source.

All aforementioned fake sink-based approaches result in excessive number of fake transmissions which is a significant overhead and causes increased link layer collisions and interfere. Fake packet generation rates are based on a fixed and predefined routing topology. Therefore, constant involvement of the BS to correct and readjust the rates in the nodes is inevitable. Moreover, introducing fake sinks only grow the number of potential adversary targets, yet the BS continues to be among these targets.

3) ROUTING TOPOLOGY OBFUSCATION

A category of countermeasures is based on disturbing the adversary's perception of the routing patterns by changing the underlying routing algorithm and/or creating shadow routes. Random walk and multi-parenting have been proposed in [15] to make the traffic pattern more disperse and make it harder for an adversary to find the BS. The approach of [58] opts to achieve source and sink anonymity by utilizing multi-path routing to create different traffic streams for image delivery. Each traffic stream is to carry a portion of the captured image. By breaking the image into different streams and rebuilding it at the destination, the network sustains anonymity without introducing much overhead. Obviously, such an approach is not well-suited for application with small sensing data. Introducing random delays in relaying packets is pursued in [27], in order to counter the time correlation of consecutive packets conducted by an adversary to analyze the traffic. Similarly, forwarding delay is used in [59] so that the traffic from a certain source is blended with traffic from other sources; however, unlike [27], the delay is determined using an open queue model. Meanwhile, L-SRA [60] uses packet buffering to equalize the same transmission rate among all nodes. It takes into account the number of active sources at a given time to set the transmission rates along the routes towards the BS. Generally, boosting the delays have major implications on the applications, especially when responsiveness is required.

FIVA [13] exploits the effect of a void on geographic routings to form a routing topology that mimics the presence of a void region surrounding the BS. Therefore, the adversary would shift its attention away from the void region that the BS is residing in. The boundary nodes of the void region are carefully selected so that their transmissions can reach the BS. The data packets are routed on the boundary of the void region and away from the BS to give the illusion that the data sink is located away from the void. In [61], the nodes close to the BS are named BLAST nodes that form a ring around the BS. BLAST nodes use K times higher transmission range compared to other nodes ($K \times t_x$) to form the BLAST ring. Thus, when a BLAST node transmits a packet, all the nodes within the ring (including the BS) receives the packet. However, for both FIVA and BLAST the number of transmissions around the void/BLAST region is quite high and can still hint at the presence of the BS. Unlike the aforementioned techniques, the approach of [16] is a link-layer rather than a network-layer

countermeasure, where the transmission power is increased. In essence such a power increase boosts network connectivity and introduces uncertainty about the next hop on the data path. Further, it exponentially grows the complexity of an adversary's ET based analysis, and ultimately elevates the BS anonymity. Obviously, sending at high power increases energy consumption of the wireless interface and rapidly drains the on-board energy supply of nodes. Our proposed AD approach overcomes this issue by being load conscious.

4) INTRODUCING COVER-UP TRAFFIC

One of the most widely used anti-traffic analysis strategies is the introduction of bogus traffic. The nature/application of the miniaturized and battery-operated nodes motivates energy conservation to prolong the network lifetime. Therefore, any traffic that does not carry useful data seems illogical. Nonetheless, Deng et al. [15] have shown that inserting fake packets from random locations with random paths, improves the BS anonymity by further confusing the adversary. A lottery model is employed to choose a neighbor to forward the fake packets to and cause local hot spots that divert the adversary's attention away from the BS. Kumar et al. [54] have proposed generating and routing fake packets over a multi-layer ring. The BS sends a fake packet to the farthest ring from its current location to trigger a fake flood within the selected ring. Bicakci et al [62] have used a flooding approach and sent each data packet not only to the sink but also to all other nodes in the network. Therefore, all nodes including the sink have equal numbers of incoming and outgoing packets. ATA [25] pursues a brute force approach to have a uniform traffic volume (transmission rate) for all nodes. Each node transmits n extra bogus packets to match its parent transmission rate, where n is determined based on the number of children that each node has. Meanwhile, PLAUDIT [18] aims at having a uniform transmission rate throughout the network. It uses a corona-based load-balanced routing tree to assign a deceptive packet rate to each node in order to equalize the traffic density across the network and make the BS undistinguishable. On the other hand, MSCLP [56] forms a clustered topology in which each cluster head (CH) transmits random fake packets that cycle within the cluster before the source node sends the real data packet.

Unlike the aforementioned node level fake packet transmission, some work employed the BS in the process. Fundamentally, the BS consumes all collected data and thus constitutes a sink in the routing topology; such a role is exploited in the traffic analysis. To improve the BS anonymity, some techniques avoid keeping the BS as a data sink and getting it involved in packet forwarding. BAR [23] gets the BS to selectively forward some of the received packets in random directions with varying time-to-live parameters in order to make the BS appear like a relay node rather than a sink. The same idea is used in [17] in a two-tier routing topology. A Hamiltonian cycle is formed in [19] to disseminate the data where the BS serves as a node in the cycle and transmit the packets that it receives.

B. COMPARISON WITH PRIOR WORK

Many of the aforementioned countermeasures demand a unique property or add a restriction to the network that narrows their applicability. For example, moving BS or deploying multiple BS is not feasible in many scenarios due to added expense. Re-routing the packet traffic to a fake node before delivery to the BS adds an unwanted delay that in time sensitive and target tracking networks are not acceptable. Approaches that intentionally or implicitly (e.g. random walk) add delay in data delivery have the same problem. While many of countermeasures from categories (I) and (III) suffer from these shortcomings, a dominant trend in categories (II) and (IV) is the generation of bogus traffic. Same nodes that generate the real data packets can generate the fake packets and therefore it is the least demanding method to design a countermeasure. Thus, many countermeasures have been exploring the idea to strategically generate fake packets that interfere with the adversary's analysis by making traffic patterns similar and the network regions indistinguishable from each other. Afterall, if all nodes and regions appear similar to the adversary, it would not be able to gain any knowledge by monitoring the network. In this work we use the same idea of fake packets to design our novel countermeasure approach, namely Assisted Deception.

To our best knowledge, published countermeasures have assumed that an adversary applies the GSAT or ET model [8], [13], [14], [17]. GSAT is solely based on traffic volume, while ET utilizes only spatial correlation of consecutive transmissions. In [27], we have introduced a more advanced approach in analyzing the network; EET. In this paper we first revisit EET and further propose a complete version that the adversary uses to incorporate temporal correlation in addition to spatial correlation. All previous countermeasures assuming ET, might have a false sense of protection against the adversary while EET is being used. In this work we show that the effectiveness of a countermeasure is negatively impacted when the adversary uses EET instead of ET. Our proposed countermeasure – Assisted Deception – is a time-correlation-aware design to have maximum impact on the adversary's EET analysis.

Moreover, the majority of published countermeasures base their design on the assumption that an adversary uses a grid model of the area while analyzing traffic, and that the cell size in such a grid is known. However, the validity of such an assumption is questionable and risks the effectiveness of the defense strategy. In addition, such a grid-based design abstracts out the nodes within the cell, ergo the countermeasure is not node-aware. Therefore, the decisions are based on cells and the overhead might be unevenly imposed on low-density and high-density cells. Obviously, such an approach could result in rapid energy exhaustion for nodes in low-density cells and could negatively impact the normal network operation. Our proposed AD countermeasure is not designed based on any assumption about grid/cell size and is indeed node-aware. Lastly, many of countermeasures require readjustment of the approach parameters based on changes in

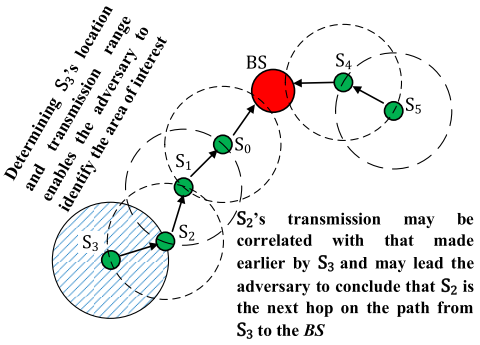

FIGURE 2. Illustrating of how transmissions are correlated to conduct traffic analysis.

the traffic pattern, nodes' load, and data routes. Such fine tuning mostly needs involvement of the BS. Any involvement of the BS has the risk of revealing its location or role. Our AD scheme is distributed and does not engage the BS in the process.

IV. ANONYMITY ASSESSMET

A. OVERVIEW OF EVIDENCE THEORY

Assessing the BS anonymity has been the focus of studies such as [8], [12]–[24], [63] and is in general a byproduct of the traffic analysis model. In this paper, ET is pursued as the underlying traffic analysis model where each intercepted transmission is deemed as an evidence of direct communication between a sender-receiver pair; the sender is determined by localizing the transmitter, while the receiver could be any node in a set of potential candidates within the sender's reachable range. Fig. 2 depicts how an adversary might analyze each transmission starting from node S_3 and trace it to the BS. The adversary estimates the sensor node's position and radio range after each transmission. The shaded area in Fig. 2 shows where the adversary is suspecting the receiver to be located at after intercepting node S_3's transmission. When node S_2 relays the packet from S_3 to next hop, the adversary locates and determines its range as shown in Fig. 2. Knowing the location and range of nodes S_3 and S_2, the adversary concludes the presence of a link relationship between the two as $(S_3 \rightarrow S_2)$. By repeating the same steps, the adversary suspects the presence of a path starting from node S_3 and ending in vicinity of BS, e.g., $(S_3 \rightarrow S_2 \rightarrow S_1 \rightarrow S_0 \rightarrow BS)$. Note that the existence and location of a receiver are unknown unless it transmits, and the adversary could intercept such transmission. Being the sink of all data, the BS does not transmit the data after receiving it from neighboring nodes, namely, node S_0 in the previous example. Therefore, the link $(S_0 \rightarrow BS)$ is just a guess that the adversary counts on.

The strength of ET comes into effect when the adversary applies the same principle on all transmissions. In our previous example, Fig. 2, we have shown another data path starting at node E. Following the path, an adversary concludes $(S_5 \rightarrow S_4 \rightarrow BS)$, and thus the adversary identifies two separate paths ending in the same region (S_3toBS, S_5toBS) and may deduce that a sink node is present in such a region. Clearly the more the number of data paths ending at the same region is, the higher the adversary's confidence in the ET analysis becomes. In Fig. 2, we are only showing nodes that are actively involved in data generation and delivery to BS. In a realistic deployment, each node might have more than one node within its reachable range, i.e., has more than one neighbor. Hence, a transmission might be directed to any of the neighbors. After detecting a transmission, the adversary revisits prior interceptions to identify a neighbor node that could have originated the previous transmission in order to correlate it with the current one. Implementing ET model in this way (node level) is possible but has following drawbacks:

1. A dense and crowded network with a great number of nodes would require major storage, and computation resources.
2. An adversary needs to be equipped with means for achieving a very accurate triangulation measurements in order to distinguish each and every node in the deployment area. Any triangulation error would result in false link assumption among sender-receiver pairs, which could degrade the effectiveness of the analysis.
3. To conclude a relationship between a pair of nodes, an adversary needs to wait for a future transmission to occur within the range of current transmission. Such a store-and-wait process not only increases the buffering requirements, but also increases the computational complexity of the analysis; considering that a next/relay transmission can be initiated by any of neighbors. Also, depending on the medium access control algorithms, packet relaying might not exactly happen in the order that the adversary expects due collisions, delays, etc. Hence, the inferred link relationships are very prone to errors.
4. An adversary collects data about the whereabouts of each node in the network, which adds yet another level of complication and difficulty. Any change like node failure, energy depletion, node movement, and node re-deployment could invalidate previously collected evidence and force the adversary to start over.
5. Depending on how the adversary eventually attacks the BS, fine-grained determination of the BS position might not be warranted. For example, radio jamming does not need to pinpoint the BS and can cover its vicinity.

A solution to overcome the aforementioned negative aspects of node level analysis is to use a grid/cell-based analysis. The adversary maps the monitored area into a grid of cells. All nodes within a cell are considered as one source. The center of a cell is considered as the position of the transmitters within the cell. Cell-based analysis addresses the drawbacks of sensor-level analysis, where:

1. All nodes inside a cell are treated as one node resulting in reduction of resource requirements.

2. Localization of senders is done at the cell level. Therefore, typical triangulation errors are more tolerable compared to node-level analysis.
3. The grid structure pre-defines neighboring cells and further simplifies the analysis. Potential destinations of each transmission can be easily determined and bounded based on range and cell size. This alleviates the need for store-and-wait.
4. Link relationships among nodes are converted to link relationships among cells. The adversary defines the grid size and knows cell relationships beforehand.
5. By setting the grid/cell size an adversary can factor in quest for launch attack against the BS, independent of sensor node density.

Fig. 3 shows a comparison between node-level and cell-level analyses. A generated packet by node S_7 is relayed over the path $S_6 \rightarrow S_5 \rightarrow S_4 \rightarrow S_3 \rightarrow S_2 \rightarrow S_1 \rightarrow S_0$ to reach BS. With a node-level analysis, the adversary is bound to track and correlate all 8 nodes and their transmissions, as indicated by Fig. 3(a). In doing so, eight links are identified. On the other hand, overlaying a grid of 3 × 3 - Fig. 3(b) - results in 4 links between cells that hold the sensors as is shown in Fig. 3(c), which constitutes 50% reduction in computational resources.

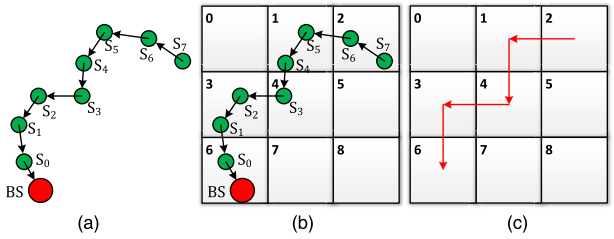

FIGURE 3. Comparing node level vs. cell level analysis. a) Node level analysis results in 8 links. b) Grid of 3 × 3 created. c) Cell level analysis results in 4 links.

B. BELIEF METRIC

The ET model for traffic analysis considers each detected transmission as an evidence of a communication link between a transmitter and a potential receiver. An adversary collects and correlates evidence in order to draw a conclusion about the existence of end-to-end communication paths. In a typical network such a process will result in a huge number of possible paths. Since the goal is to locate BS, all paths in the final set are not of the same importance. Also, some concluded paths might be wrong due to errors in the evidence correlation process. In order to weigh paths against each other and filter out any noise from the final set, ET defines path-based evidence as shown in (1). Evidence for a path between two nodes equals the minimum evidence available on the individual links on such a path.

$$PE\,(L) = \min_{U \subseteq L} E\,(U)\,, \quad |L| \geq 2 \tag{1}$$

Equation (2) shows normalized version of (1)

$$PE_{norm}\,(L) = \frac{PE(L)}{Total\ Evidence} \tag{2}$$

Total evidence is equal to the sum of all evidence that an adversary has collected and derived. The normalized value of evidence expresses the proportion of each claimed path to all possible paths. D. Haung [12] further introduced a *Belief* function for representing the anonymity of a node x based on the evidence for the set of paths P ending at x:

$$Bel\,(x) = \sum_{L|L \subseteq P} PE_{norm}\,(L) \tag{3}$$

The *Belief* reflects the adversary's confidence that a node x is the end point of a path P. Equation (4) shows normalized version of (3)

$$Bel_{norm}\,(x) = \frac{Bel(x)}{Total\ Beleif} \tag{4}$$

The normalized *Belief* carries the same intuition of normalized evidence; it expresses the proportion of each *Belief* relative to rest of *Beliefs*. The total *Belief* is the sum of all *Belief* values. In the next subsection, an elaborate example demonstrates the steps that an adversary takes while employing ET to locate BS.

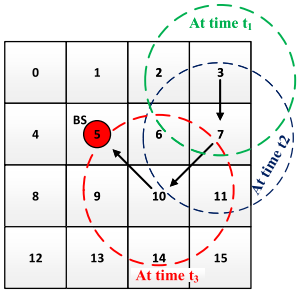

FIGURE 4. Initial data transmission at t_1. At t_2 and t_3, data is relayed towards BS.

C. ILLUSTRATIVE EXAMPLE

The applicability of ET is illustrated using a detailed example. For simplicity, we assume a 4 × 4 grid. As shown in Fig. 4, the sensor node in cell #3 generates and transmits the first data packet at time t_1 which is destined to the BS at cell #5. Upon intercepting such a transmission, the adversary considers it as a link evidence between cell #3 and all neighboring cells; cells #2, #6, and #7 in Fig. 4. Table 1 shows the state of the adversary's evidence table after t_1. In Fig. 4, one possible route from cell #3 to cell #5 is shown. Such a route uses cell #7 at time t_2, and cell #10 at time t_3 as relay cells to deliver the data originated at cell #3 to the BS in cell #5. Table 2 and Table 3 show the state of the adversary's evidence table after t_2 and t_3, respectively.

Fig. 5 shows the same example with the addition of a second data route starting at cell #0 and ending at cell #5. The adversary applies the same method as before in collecting

TABLE 1. Evidence table at t_1.

Relation	Evidence
$3 \rightarrow 2$	1
$3 \rightarrow 6$	1
$3 \rightarrow 7$	1

TABLE 2. Evidence table at t_2.

Relation	Evidence
$3 \rightarrow 2$	1
$3 \rightarrow 6$	1
$3 \rightarrow 7$	1
$7 \rightarrow 2$	1
$7 \rightarrow 3$	1
$7 \rightarrow 6$	1
$7 \rightarrow 10$	1
$7 \rightarrow 11$	1

TABLE 3. Evidence table at t_3.

Relation	Evidence
$3 \rightarrow 2$	1
$3 \rightarrow 6$	1
$3 \rightarrow 7$	1
$7 \rightarrow 2$	1
$7 \rightarrow 3$	1
$7 \rightarrow 6$	1
$7 \rightarrow 10$	1
$7 \rightarrow 11$	1
$10 \rightarrow 5$	1
$10 \rightarrow 6$	1
$10 \rightarrow 7$	1
$10 \rightarrow 9$	1
$10 \rightarrow 11$	1
$10 \rightarrow 13$	1
$10 \rightarrow 14$	1
$10 \rightarrow 15$	1

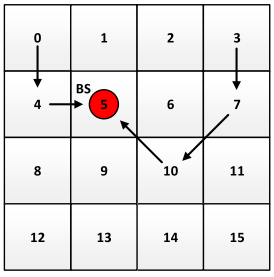

FIGURE 5. Routing topology with two paths ending at BS.

evidence based on the observed transmissions and possible links between cells. Table 4 shows the final state after both transmissions have reached the BS, i.e., cell #5. In order to apply ET on the collected evidence, the adversary derives new paths/links based on the collected ones which are shown in Table 4. For example, based on the evidence $(3 \rightarrow 7)$, $(7 \rightarrow 10)$, and $(10 \rightarrow 5)$, the adversary derives the path $(3 \rightarrow 7 \rightarrow 10 \rightarrow 5)$. Note that in this process, paths like $(3 \rightarrow 7 \rightarrow 6)$, $(3 \rightarrow 7 \rightarrow 10 \rightarrow 15)$, $(0 \rightarrow 4 \rightarrow 5)$, $(4 \rightarrow 0 \rightarrow 5)$, and many more are derived. In this example, after the adversary derives all possible paths, the total number is 56 paths.

TABLE 4. Evidence table after both transmissions reach BS.

Relation	Evidence
$3 \rightarrow 2$	1
$3 \rightarrow 6$	1
$3 \rightarrow 7$	1
$7 \rightarrow 2$	1
$7 \rightarrow 3$	1
$7 \rightarrow 6$	1
$7 \rightarrow 10$	1
$7 \rightarrow 11$	1
$10 \rightarrow 5$	1
$10 \rightarrow 6$	1
$10 \rightarrow 7$	1
$10 \rightarrow 9$	1
$10 \rightarrow 11$	1
$10 \rightarrow 13$	1
$10 \rightarrow 14$	1
$10 \rightarrow 15$	1
$0 \rightarrow 1$	1
$0 \rightarrow 4$	1
$0 \rightarrow 5$	1
$4 \rightarrow 0$	1
$4 \rightarrow 1$	1
$4 \rightarrow 5$	1
$4 \rightarrow 8$	1
$4 \rightarrow 9$	1

This example only assumes two transmissions. For simplicity, routes are picked to not share any common cells and also not have any adjacent cells. Consequently, as Table 1 through Table 4 show, the value for each link/evidence is 1. Applying (1) on the observed and derived paths results in *PE* value of 1 for each path. Since the number of all observed and derived paths are 56, the Total Evidence equals to 56. Hence, based on (2), PE_{norm} for each path is 1/56.

The next step is to calculate the *Belief* measure for each cell using (3). For demonstration purposes, cell #5 (location of BS) is shown here. Table 5 shows all paths ending at cell #5 with their corresponding evidence, normalized evidence, the number of subsets, and the corresponding *Belief* measure. Note that (3) includes all subsets of a given path. Hence for a path like $(3 \rightarrow 7 \rightarrow 10 \rightarrow 5)$, six subsets of $(3 \rightarrow 7)$, $(7 \rightarrow 10)$, $(10 \rightarrow 5)$, $(3 \rightarrow 7 \rightarrow 10)$, $(7 \rightarrow 10 \rightarrow 5)$, and $(3 \rightarrow 7 \rightarrow 10 \rightarrow 5)$ exists that results in a *Belief* measure of 6/56.

After calculating the *Belief* measure of all cells, the final step is to calculate the normalized *Belief* for each cell using (4). The result of this step is shown in Fig. 6. The cell with the highest normalized *Belief* value, i.e., cell #6, is the best guess of the adversary for the BS location. Obviously, this is not the right cell; however, it is a very good guess considering that only two transmissions (two paths) are used to draw the conclusion. The actual location of the BS (cell #5) has the second highest value, which demonstrates the effectiveness of ET. The detection accuracy would grow by intercepting more transmissions and collecting more evidence.

ET uses statistical analysis to collect data and derive new evidence based on its observed transmissions, which makes it inevitable to derive a long and insignificant path from observed relations. To elaborate, let us assume a new

TABLE 5. Belief table for paths ending at cell #5.

Paths ending at cell 5	Evidence	E_{norm} (total = 56)	# of subsets	*Belief* value of each path
$0 \rightarrow 5$	1	1/56	1	1/56
$4 \rightarrow 5$	1	1/56	1	1/56
$0 \rightarrow 4 \rightarrow 5$	1	1/56	3	3/56
$4 \rightarrow 0 \rightarrow 5$	1	1/56	3	3/56
$10 \rightarrow 5$	1	1/56	1	1/56
$7 \rightarrow 10 \rightarrow 5$	1	1/56	3	3/56
$3 \rightarrow 7 \rightarrow 10 \rightarrow 5$	1	1/56	6	6/56
Belief in BS being at cell #5				18/56 ~ 0.321

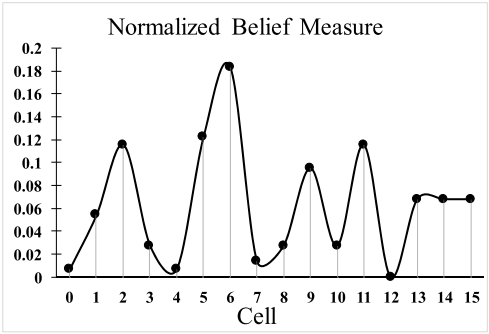

FIGURE 6. Detectability/*Belief* measure in illustrative example. A higher value indicates higher confidence of adversary about the BS presence in corresponding cell.

transmission in Fig. 5 that originates from cell #13 and reaches the BS via cell #9. The transmission from cell #13 adds $(13 \rightarrow 8)$, $(13 \rightarrow 9)$, $(13 \rightarrow 10)$, $(13 \rightarrow 12)$, and $(13 \rightarrow 14)$ to ET table while the transmission from cell #9 adds $(9 \rightarrow 4)$, $(9 \rightarrow 5)$, $(9 \rightarrow 6)$, $(9 \rightarrow 8)$, $(9 \rightarrow 10)$, $(9 \rightarrow 12)$, $(9 \rightarrow 13)$, and $(9 \rightarrow 14)$. When the adversary derives new links/paths based on its collected data, from $(3 \rightarrow 7)$, $(7 \rightarrow 10)$, $(10 \rightarrow 9)$, $(9 \rightarrow 13)$, and $(13 \rightarrow 12)$, the path $(p_1 : 3 \rightarrow 7 \rightarrow 10 \rightarrow 9 \rightarrow 13 \rightarrow 12)$ emerges. Obviously, such a path does not assist the adversary in identifying the location of the BS. Note that the length of the path is 5 and is longer than the valid paths $(13 \rightarrow 9 \rightarrow 5)$ and $(3 \rightarrow 7 \rightarrow 10 \rightarrow 5)$. Thus, we believe that any modification of ET and its *Belief* measure based on the length of a derived path might introduce error and falsify the statistical significance of said path. Therefore, in this paper we do not use the weighted *Belief* measure that has been adopted in recent work [17]–[23], [27], [63].

V. ENHANCED EVIDENCE THEORY (EET)

In this section we present our novel traffic analysis model that extends the capabilities of ET and better reflects the threat that a WSN network is subject to. In the next section we propose effective countermeasure that safeguards the WSN against such novel and effective attach model.

A. TEMPORAL CORRELATION OF INTERCEPTED TRANSMISSIONS

The goal of an ET-based attack is to identify data paths ending at the BS. It is founded on intercepting transmissions and correlating them to infer communication links. Specifically, spatial correlation is applied by factoring in the source location and transmission range. We propose an EET model that utilizes temporal correlation in addition to spatial correlation. In a WSN, nodes relay incoming packets as soon as possible to minimize packet-delivery delay and prevent queue fill-up which can result in packet drops. Therefore, there is a high probability that an incoming packet is relayed in a short time window after reception. Thus, spatially correlated transmissions could also benefit from considering temporal factors if they occur consecutively in a short time window. Among all spatially correlated cells, a temporally correlated pair of cells is more likely to reveal the actual routing path.

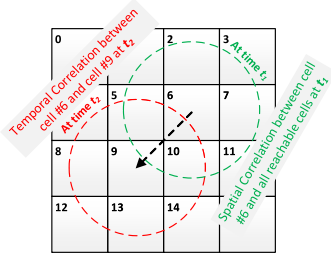

FIGURE 7. Temporal vs. Spatial Correlation.

Let us look at the example shown in Fig. 7. At t_1, a transmission from cell #6 is originated. Based on the detected range, spatial correlation among cell #6 and its neighboring cells are formed that are recorded as $(6 \rightarrow 1)$, $(6 \rightarrow 2)$, $(6 \rightarrow 3)$, $(6 \rightarrow 5)$, $(6 \rightarrow 7)$, $(6 \rightarrow 9)$, $(6 \rightarrow 10)$, and $(6 \rightarrow 11)$. When at $t_2 < \Delta T$ a second transmission originates from cell #9, there is a high possibility that such a transmission is relaying the data that earlier was sent from cell #6. Therefore, a temporal correlation of $(6 \rightarrow 9)$ is warranted. Such a temporal relation boosts confidence of an observer in predicting the routing path. Prior to t_2, the adversary has the record of $(6 \rightarrow 9)$ in its table. To signify its importance in comparison to other spatially-correlated links in the table, we propose adding a bonus value to the evidence corresponding to $(6 \rightarrow 9)$. Fig. 8 shows a case in which cell #5 and cell #11 both are transmitting at t_2. In these circumstances there are more than one possible temporal relations; we take a conservative approach and do not include any bonus for any of possible links; in this example $(6 \rightarrow 5)$ and $(6 \rightarrow 11)$.

To Illustrate, let us reconsider the example in Fig. 4 while applying EET. The first and second transmissions at time t_1 and t_2 populate the adversary's table in a similar way to

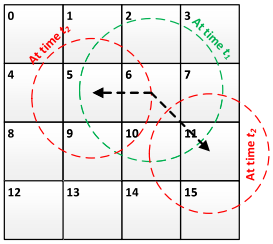

FIGURE 8. Two candidates for Temporal Correlation.

TABLE 6. Evidence table at t_2 when EET is applied.

Relation	Evidence
3 → 2	1
3 → 6	1
3 → 7	1+bonus
7 → 2	1
7 → 3	1
7 → 6	1
7 → 10	1
7 → 11	1

TABLE 7. Evidence table at t_3 when EET is applied.

Relation	Evidence
3 → 2	1
3 → 6	1
3 → 7	1+bonus
7 → 2	1
7 → 3	1
7 → 6	1
7 → 10	1+bonus
7 → 11	1
10 → 5	1
10 → 6	1
10 → 7	1
10 → 9	1
10 → 11	1
10 → 13	1
10 → 14	1
10 → 15	1

what is shown in Table 1 and Table 2. Though this time since the adversary is using EET, it also temporally correlates the transmissions of cell #7 and cell #3. To reflect the temporal relation, the adversary updates the evidence table with an added bonus for link (3 → 7) as shown in Table 6. After t_3, time correlation is observed between the transmissions of cell #10 and cell #7, in addition to other spatial correlations. Therefore, the adversary allocates a bonus to (7 → 10), as shown in Table 7.

The effect of the second route (0 → 4 → *BS*) from Fig. 5, is reflected in Table 8. Other than the added bonus to temporally correlated transmission, the EET model stays the same as ET; i.e. deriving new paths/links, and then calculating total evidence, normalized evidence, *Belief*, and normalized *Belief*. Fig. 9 shows the curve of normalized *Belief* when different bonus values are used. A bonus of zero makes EET similar to ET and causes cell #6 to have the highest value. By choosing a bonus value of 5 or 20, the confidence in cell #6 is lowered, yet cells #6 still has the highest *Belief*.

TABLE 8. Evidence table after both transmissions reach BS.

Relation	Evidence
3 → 2	1
3 → 6	1
3 → 7	1+bonus
7 → 2	1
7 → 3	1
7 → 6	1
7 → 10	1+bonus
7 → 11	1
10 → 5	1
10 → 6	1
10 → 7	1
10 → 9	1
10 → 11	1
10 → 13	1
10 → 14	1
10 → 15	1
0 → 1	1
0 → 4	1+bonus
0 → 5	1
4 → 0	1
4 → 1	1
4 → 5	1
4 → 8	1
4 → 9	1

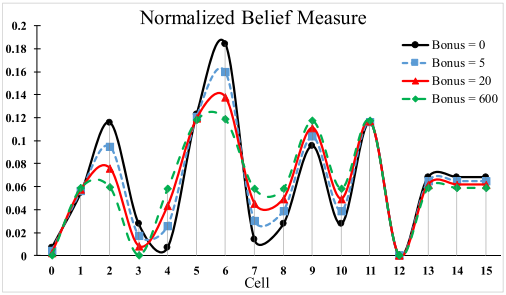

FIGURE 9. *Belief* Measure with different bonus value in EET Model where the BS is located in cell #5 in a 4 × 4 grid.

By setting the bonus to 600, both cell #6 and cell #5 have the same *Belief* measure and thus the adversary may choose to attack both cells at once. The BS is in cell #5 and any attack on the cell impacts the network capability and hence means attack success. Note that this is a simple example with only two routes ending at the BS. Therefore, selection of bonus value was exaggerated to demonstrate its effect. In the next subsection, the selection of bonus value is analyzed in detail.

B. BONUS VALUE SELECTION

EET utilizes temporal correlation of transmissions while ET only relies on spatial correlation. EET adds a bonus value to entries in the evidence table that are temporally correlated, to signify the importance of those links. The bonus value can impact the effectiveness of EET which elevates the criticality of bonus value selection.

1) STATIC (FIXED) BONUS SETTING

As pointed out earlier, in Fig. 9 the BS location, specifically cell #5, does not have the highest *Belief* when the bonus value

is 0, 5, or 20, and consequently is not the top choice for the attacker. However, with a bonus value to 600, both cell #5 and cell #6 would have the highest normalized *Belief* value, which means the anonymity of BS is compromised. To further demonstrate the importance of bonus value selection, EET model with a wide range of bonus values were applied to three randomly generated topologies in a 8 × 8 grid setup. Fig. 10 shows the rank of the BS cell for each bonus value. Note that lower rank means that the cell has higher normalized *Belief* measure. Therefore, lower rank is equivalent to lower BS anonymity and higher BS detectability.

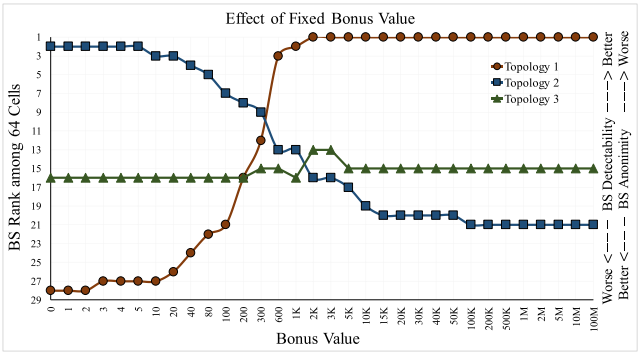

FIGURE 10. Impact of bonus value on BS anonymity in three different topologies.

In Topology #1, a bonus value of zero makes the BS cell to be ranked #28 out of 64 cells. By increasing the bonus value, the rank of the BS cell starts to lower, which means it is becoming more detectable and its anonymity is worsening. With a bonus value of 2K, the BS cell is ranked #1 and becomes the adversary's prime pick for attack. Any bonus value greater than $2K$ is not changing the curve. From the adversary's perspective, bonus values of 2K or greater are an excellent choice since it results in successfully identifying the cell that the BS is located at. Yet, Fig. 10 shows a different behavior for the second topology. Bonus values less than 5 result in BS rank of #2. By growing the bonus, the BS anonymity is improving rather than diminishing unlike the case of Topology #1. Despite being a good selection in Topology #1, a bonus value of 2K yields 8 folds of decrease in the adversary's capability to detect the BS in Topology #2. On the other hand, the *Belief* curve for Topology #3 shows only minor fluctuations for the different bonus values. Overall, Fig. 10 clearly indicates that the best bonus value is dependent on the topology under surveillance. Therefore, pursuing a fixed bonus value is not an appropriate approach. Hence, we pursue an adaptive approach for setting the bonus value.

2) DYNAMIC BONUS VALUE

In the ET model, the evidence for a link L that represents $C_i \rightarrow C_j$ reflects the number of times a transmission from C_i reaches C_j. The EET model, on the other hand, factors in temporal correlation when a transmission is made from C_j within a time window ΔT after C_i. Inference of temporal dependence is captured by adding a bonus (bias) to the evidence of link L. Thus, in the EET model the evidence of L can be expressed as:

$$\begin{aligned} Evidence_{EET}\,(L) = {} & Evidence_{ET}\,(L) \\ & + Temporal\ Evidence\,(L) \\ & \times Bonus\ Value \end{aligned} \tag{5}$$

In the previous section we have highlighted the challenge for selecting an effective bonus value. $Evidence_{ET}\,(L)$ is based on the adversary's perspective and represents confidence in the presence of a link L; hence we propose to use it as the bonus value for $TemporalEvidence\,(L)$. Such an approach makes the increased evidence, i.e., bonus value, proportional to adversary's current confidence level. We note that the problem in using a fixed bonus is that the impact may mislead the analysis since it could allow temporal relations to dominate the results of spatial correlation and eventually leads the analysis to the wrong conclusion. For example if a link has a low $Evidence_{ET}$, using a fixed and large bonus value changes the evidence radically; similar to behavior of Topology #1 in Fig. 10. Choosing $Evidence_{ET}$ as the bonus value makes it adaptable. By rewriting (5), we arrive at:

$$\begin{aligned} Evidence_{EET}\,(L) = {} & Evidence_{ET}\,(L) \\ & + Temporal\ Evidence\,(L) \\ & \times Evidence_{ET}\,(L) \end{aligned} \tag{6}$$

The effectiveness of our adaptive bonus setting approach is inevitable when (6) is used for the topologies of Fig. 10. The best outcome for an adversary is when using a bonus value greater than 2K for Topology #1 and less than 5 for Topology #2, which results in a BS rank of 1 and 2, respectively. When setting the bonus dynamically based on (6), the BS rank becomes consistent with the best fixed bonus as shown in Fig. 11. For Topology 3, the fixed bonus value did not change BS rank considerably; yet with the adaptive setting the BS rank becomes more indicative, where the dynamic bonus value results in a BS rank of 4 which constitutes 3 times improvement in BS detectability.

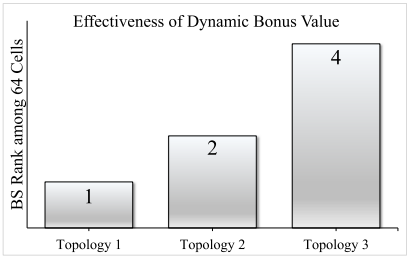

FIGURE 11. BS anonymity when Dynamic Bonus Value is used.

C. TIME WINDOW (ΔT)

In EET, cells C_i and C_j are temporally correlated if a transmission initiated at t_1 within cell C_i can reach C_j and a subsequent transmission at t_2 follows from within C_j, where

$t_2 - t_1 \leq \Delta T$. In this section we study how an adversary may select ΔT. In a typical multi-hop network, a store-and-forward strategy is applied where nodes often store incoming packets in a FIFO queue and attempt to transmit them in the same order, as fast as possible. Especially in time sensitive and real-time applications, such an approach is necessary to minimize packet delivery delay and maximize network throughput. Moreover, the duty cycle of sensors is typically long enough to allow all packets to reach the BS before the next duty cycle starts. When there are no packets in the queue, an incoming packet is transmitted immediately after reception. If there are n packets in the queue, the incoming packet is sent out after all n pending packets are transmitted. Therefore, the time until transmitting is:

$$Queuing\ Time = n \times \tau, \tag{7}$$

where τ is the transmission duration for a packet in *ms* and is calculated by dividing data packet size by the channel bit rate. The adversary can estimate τ by sampling transmission bursts across the network and measuring their duration. On the other hand, the adversary does not have insight on the network topology and hence cannot predict the average queue length to estimate n. Furthermore, the adversary uses a grid model to monitor and analyze the network. All transmissions within a given cell are assumed to be made from the cell center regardless of the node density of the cell. In other words, from an adversary's perspective the number of nodes is equal to the number of cells, and hence a cell has incoming packets that at most is equal to the number of its neighbors. EET uses the average number of neighbors as an estimate of n.

A given cell in a grid falls into one of three categories: corner, edge, or internal cell. By considering the number of cells in each category and the number of neighboring cells per category, we can arrive at the average number of neighbors. In an $M \times M$ gird, the number of corner cells is always 4. Each edge consists of M cells, two of which are corner cells. Therefore, each edge only has $(M - 2)$ edge cells. Thus, the total number of edge cells is:

$$(M - 2) * 4 = 4M - 8 \tag{8}$$

The number of internal cells is total number of cells minus edge and corner cells:

$$M^2 - ((4M - 8) + 4) = M^2 - 4M + 4 \tag{9}$$

A corner, edge, and internal cell has 3, 5 and 8 neighboring cells, respectively. Putting together the cell count for each category and the number of neighbors per category, we arrive at a total number of neighbors for a grid of $M \times M$ as:

$$\begin{aligned}&(4 * 3) + ((4M - 8) * 5) + (\left(M^2 - 4M + 4\right) * 8)\\ &\quad = 8M^2 - 12M + 4\end{aligned} \tag{10}$$

Dividing (10) by the number of grid cells ($M \times M = M^2$):

$$Average\ Number\ of\ Neighbors = \frac{\left(8M^2 - 12M + 4\right)}{M^2} \tag{11}$$

Back in (7), n can be substituted for by (11) which results in:

$$time\ to\ transmit = \frac{\left(8M^2 - 12M + 4\right)}{M^2} \times \tau \tag{12}$$

Equation (12) is based on the assumption that only one transmission is initiated from each cell. If the node density in cells is $d > 1$, the number of transmissions is equal or greater than d, depending on their relative location and routing path. By incorporating the density factor, d, in (12), we have:

$$time\ to\ transmit = \frac{\left(8M^2 - 12M + 4\right)}{M^2} \times d \times \tau \tag{13}$$

The value of d can be estimated in multiple ways. For example, the adversary could survey a number of cells either by using in-situ trackers or by using extra global eavesdroppers to identify individual nodes within the cells using RF fingerprinting. Note that this step does not need an accurate localization technique if the approach can distinguish between unique transmitters. Another approach would be to average the number of transmissions originated from a subset of cells to arrive at a rough estimate of the value of d. If the adversary has an insight knowledge of the network deployment and potential sensors counts, another option is to estimate d by dividing the sensor count by the grid size.

Equation (13) provides an average estimate on the time to transmit for a given packet. In EET, ΔT can simply be set to same value, i.e.,

$$\Delta T \approx \frac{\left(8M^2 - 12M + 4\right)}{M^2} \times d \times \tau \tag{14}$$

We have conducted a simulation using a 10×10 grid setup with 200 nodes, $2Kbit$ data packets, and $2Mbps$ channels. Thus, $d = \frac{200}{100} = 2$, and $\tau = \frac{\text{Data Packet Size}(10Kbits)}{\text{Data Transmission Bit Rate}(2Mbps)} = 5ms$. Using (14), we have:

$$\Delta T \approx \frac{(8 \times 10^2 - 12 \times 10 + 4)}{10^2} \times 2 \times 5ms = 68.4ms$$

The simulation opts to gauge the impact of ΔT and the effectiveness of (14). Based on the simulation results shown in Fig. 12, one can note that increasing ΔT reduces the total number of temporal correlations performed by EET. As expected, when ΔT grows, the number of transmissions that are triggered within a time window increases, which introduces uncertainty for which of these transmissions may be temporally correlated by EET. Fig. 12 indicates that the adversary should use a very small ΔT (e.g. *10 ms*) to achieve the best outcome. In Fig. 12 we have shown the number of "Correct" and "Wrong" time correlations. Clearly, variation of ΔT impacts those numbers as well. In Fig. 13 we have shown the proportion of "Correct" and "Wrong" time correlations in respect to the total count. Fig. 13 shows that a ΔT of 10ms results in more "Wrong" correlations. As ΔT increases, the proportion of "Correct" correlations increases in respect to the "Wrong" ones. Specifically, $\Delta T = 70ms$ gives the highest value which is a very close approximation of the value that (14) suggests.

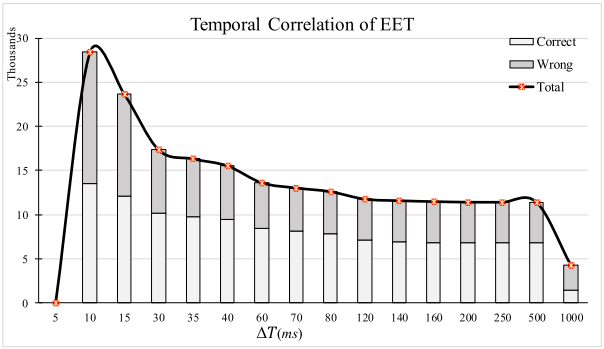

FIGURE 12. Number of Correct and Wrong temporal correlations in respect to ΔT.

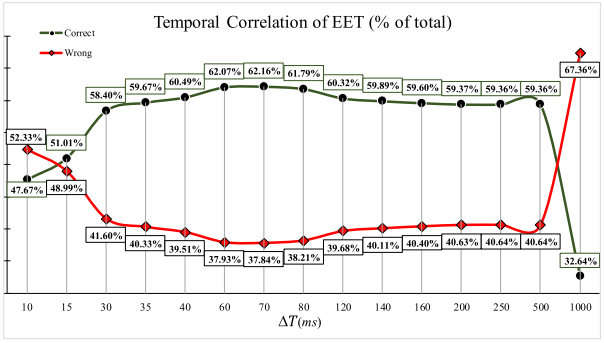

FIGURE 13. Correct and Wrong temporal correlations in respect to the total correlations.

VI. ASSISTED DECEPTION COUNTERMEASURE

In [27] we have proposed DPR to counter EET-based attacks. DPR is a passive defense mechanism in which each node adds delay in relaying an incoming data packet to interfere with time correlation of consecutive transmissions. Due to added delay, DPR is only viable for applications that can tolerate tardy packet delivery. In this section, we present our novel AD mechanism, which counters EET and does not increase the data packet latency. AD can be used even if the adversary is not pursuing EET as an attack model; in Section VII, we show that AD increases the anonymity of BS under both ET and EET.

A. DECEPTED PACKETS GENERATION

As the name indicates, in our Assisted Deception mechanism, neighboring nodes assist each other to cover up temporal relationships among transmissions by timely injecting deceptive packets. Quite a few published studies, e.g. [15], [22], [24], [63]–[66], have used fake/deceptive packets as a means for disturbing the spatial correlation of packets and boosting the BS anonymity. Unlike these approaches, AD targets both spatial and temporal correlation of intercepted data packets by coordinating the times at which deceptive packets are transmitted. Before discussing the details of how deceptive packets are generated, we illustrate the idea through an example.

1) BASIC IDEA

Fig. 14(a) shows a typical network that has no defense mechanism in place. An observer can employ EET to time correlate each transmission to the next one and deduce the route ($S_2 \rightarrow S_1 \rightarrow S_0$). Fig. 14(b) shows the same network when AD has been employed. Node S_2 transmits its packet at t_1, which is destined to S_1. Node S_3 happens to be the neighbor of S_2 that overhears the transmission. In a typical scenario, node S_3 ignores the packet that is not destined to it. However, in AD the data packet sent by node S_2 has extra fields to inform node S_3 that it has been chosen as a designated cover-up transmitter. Therefore, node S_3 sends a deceptive packet at time t_2 at which node S_1 is relaying the data packet to its next hop, namely, node S_0. Hence, an observer sees two transmissions taking place simultaneously at t_2 which results in two possible temporal relationships: $S_2 \rightarrow S_1$ and $S_2 \rightarrow S_3$. As discussed in Section VI and shown in Fig. 8, an adversary that uses EET does not use either of the evidence in its analysis due to imposed uncertainty.

In Fig. 14(c) we depict another scenario in which node S_1 transmits ε time units after t_2. Since node S_3 transmits its deceptive packet earlier at t_2, the adversary deems $S_2 \rightarrow S_3$ as the temporal evidence instead of real one which is $S_2 \rightarrow S_1$. Hence, AD not only prevents deduction of $S_2 \rightarrow S_1$, but also introduces wrong evidence into the adversary's analysis. Fig. 14(d) shows a third scenario in which node S_3 transmits after S_1, implying that $S_2 \rightarrow S_1$ is deduced. Thus, in this scenario, AD is not successful in hiding the relationship between S_2 and S_1. Nonetheless, the deceptive packet of S_3 constitutes an extra transmission that the adversary needs to observe and track. Such extra transmission contributes to boosting the traffic volume and is most likely to be correlated to other real or deceptive packets, resulting in more confusion for the adversary.

2) SELECTING FAKE PACKET TRANSMITTER

The following terms are used in explaining AD

- *Cover-up Node*: the sensor that is tasked to transmit a deceptive packet simultaneously with another node. For example, node S_3 is a cover-up node for S_1's transmission in Fig. 14(b).
- *Trigger Node:* the node that decides which among its neighbors acts as a cover-up node. For example, node S_2 is a trigger node in Fig. 14(b).

To distinguish between data and deceptive packets, AD adds two custom fields to the packet header, namely, cover-up ID and fake flag. The former identifies the node that has been chosen by the current transmitter to play the role of cover-up node. Meanwhile, the fake flag is used to mark deceptive packets and distinguish them from a real data packet. Each trigger node picks a cover-up node among its neighbors based on the following criteria:

- *Criterion #1*: In order to minimize overlap and possibility of medium access collision, a trigger node S_i favors a cover-up S_j that is the farthest from node S_i's next hop on the data route to the BS.

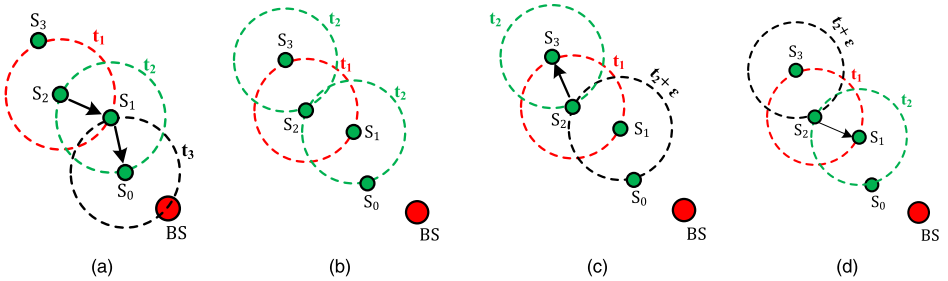

FIGURE 14. Illustrating the operation of the Assisted Deception approach; a) Assisted Deception is not applied; b) first scenario where data and deceptive packets are transmitted simultaneously at t_2; c) second scenario where the data packet is transmitted after the deceptive packet; d) third scenario when the data is transmitted before the deceptive packet.

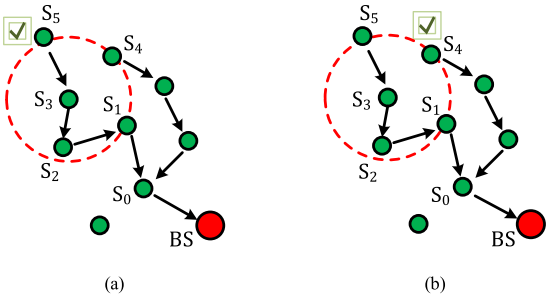

FIGURE 15. Illustrating the section of the cover-up node by sensor node S3; (a) Node S5 is the farthest neighbor from next hop S2; (b) Cover-up node, S4, is not on the same route with trigger node S3.

- *Criterion #2:* The next hop of the cover-up node must not be the trigger node.

To demonstrate and explain each criterion, let us use the example in Fig. 15 with trigger node S_3. Node S_3's next hop is node S_2. Among node S_3's neighbors, node S_5 is the farthest from S_2. Therefore, S_5 satisfies *Criterion* #1 (Fig. 15(a)). A closer look at the route setup reveals that nodes S_5, S_3, and S_2 are all on the same data dissemination path. In other words, S_5's next hop happens to be S_3. Thus, any transmission from S_5, either data or deceptive packet, might be considered by the adversary as evidence for $S_5 \rightarrow S_3$, and positively rather than negatively affect the traffic analysis attack. Therefore, our AD approach qualifies the selection using *Criterion* #2 and picks node S_4 as a cover-up, as shown in Fig. 15(b). In case the adversary correlates the transmission of S_4 and S_3, it would not be a valid link and determent the adversary's analysis. The selection of a cover-up node is done as a part of real data transmission from $S_3 \rightarrow S_2$. In our example, nodes S_5 and S_4 both overhear S_3's transmission. If a neighbor finds the cover-up ID matches its own and the fake indicator is false in the packet, such a neighbor generates the deceptive packet during the next time window.

3) FAKE TRAFFIC GENERATION

By timely transmission of deceptive packets, AD is aiming to falsify the temporal correlation analysis. AD marks the deceptive packets with a fake flag and hence nodes can easily identify them. In its simplest form, AD directs the nodes to ignore deceptive packets and do not route them. We call this *Pulse mode* and refers to it as AD-P. Alternatively, fake packets could be further routed beyond the cover-up node. We refer to that as AD *Routed mode*, or AD-R for short. Naturally, routing of fake packets results in a higher number of deceptive transmissions in the network. If directed away from the BS, such extra transmissions have the obvious benefits of: (i) increasing overall traffic volume of the network which boosts the complexity of the ET and EET analysis [15], and (ii) getting the adversary to consider irrelevant links and false paths because of the indistinguishability between real and deceptive packets for someone who cannot decode the intercepted transmission.

The selection between pulse and routing modes depends on the energy and anonymity implications. While routing deceptive packets has a positive effect, it could potentially shorten the lifespan of the involved nodes or if not carefully planned could degrade the BS anonymity. Regions closer to BS tend to have higher transmission rates because of the multi-hop data packet relaying. Transmitting deceptive packets might thus accelerate energy consumption in these regions. As explained in the next subsection, AD-R picks a route that minimizes time to live of deceptive packets in regions closer to BS. Thus, the energy overhead and impact of traffic volume are kept at minimum. To minimize the impact of deceptive transmissions on delivery of data packets, each node has to designate a separate queue for fake packets with lower priority. Deceptive packets are inserted into a low priority queue and are transmitted only if the data packet queue is empty.

When pursued, AD-R, utilizes a smart routing technique to further increase the benefits of the extra transmissions in the network. By routing deceptive packets away from BS, the traffic volume increases in regions far from BS and makes it harder for the adversary to distinguish the vicinity of BS from other areas. In addition, it also causes the illusive presence of multiple data sinks (base-stations) in the network. To achieve the latter, for each trigger-node, deceptive packets are routed away from BS and up to the same number of hops. Fig. 16 shows an example to demonstrate the idea.

The data from trigger node S_i reaches BS in 4 hops. Therefore, the deceptive packet is routed four times and reaches to node S_j. To an observer, either route ($S_i \rightarrow BS$ *or* $S_i \rightarrow S_j$) is a valid path that could imply a final destination. On the other hand, AD-P does not route deceptive packets and hence, in example of Fig. 16 the path ($S_i \rightarrow S_j$) never forms under AD-P.

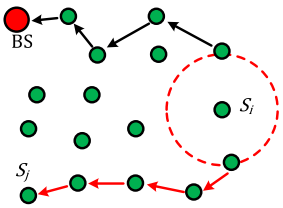

FIGURE 16. AD-R routes the deceptive packet to Sj and gives the illusion of two BS.

B. ROUTING OF DECEPTIVE PACKETS

AD is a decentralized defense mechanism that intends to have minimum setup requirement and involvement from the BS. Therefore, to disseminate the deceptive packets in Routing mode of AD (AD-R), we propose to use random next hop selection which is a simple routing algorithm with minimum overhead [15]. One known drawback of random selection is the route length unpredictability which results in unfavorable latency. Nonetheless, AD is using it only to route deceptive packets and not the data packets. Therefore, such a drawback is not a concern in the context of AD. However, if left without constraints, the use of random function to select the next hop could result in deceptive packets being routed toward BS or indefinitely. Clearly those circumstances defy the purpose of injecting deceptive packets in the network as discussed earlier. Hence, AD sets the following rules that each node complies with while handling deceptive packets:

- *Rule 1 – Direction Control*: We define a level of a node as the number of hops on its shortest path to BS. Immediate BS neighbors can reach it directly and have a level of 0; a node that reaches the BS via one relay would have a level of 1, and so forth. Levels are often determined during data route setup. Deceptive packets are routed only to a neighbor node that has the same or higher-level value. This constraint ensures that deceptive packets are not routed towards the BS. At the same time, it allows for deceptive packets to travel among same level nodes.
- *Rule 2 – Controlled Overhead*: A new time-to-live (*TTL*) field is added to the packet header to ensure that deceptive packets die off after a certain number of transmissions. Upon receiving a deceptive packet, a node decrements the *TTL* field by one. If *TTL* becomes zero, the deceptive packet is discarded.

1) TTL SETTING

A node at level n reaches the BS after 1 initial data transmission and n relay transmissions; resulting in a total of $1+n$ transmissions. In the first data transmission, the trigger node informs the designated cover-up, which generates one deceptive packet to be routed for total of $(n-1)$ times within the network; resulting in n deceptive transmissions corresponding to n data relay transmissions. Therefore, AD sets the initial *TTL* value to match the level of the trigger node, i.e. n. One could argue that a deceptive packet with a large *TTL* might reach to the network edge quickly and never exhaust its *TTL* value. However, AD allows deceptive packets to travel among nodes on the same level, and hence a deceptive packet that has reached to the edge of the network has the opportunity to travel on the network periphery until its *TTL* reaches zero. A special case is when an edge node has no neighbors to route the deceptive packet to. We refer to such a node as a terminal, which in essence is a leaf in the network. In AD, a terminal node has the following three options for handling a deceptive packet that has *TTL* greater than zero:

i) *Drop*: The terminal node drops the packet if it does not have any neighbor node that fulfills *Rule #1*.
ii) *Single Beat*: The terminal node transmits one deceptive packet without setting the recipient field. In other words, a deceptive packet is transmitted only once when it reaches a terminal node.
iii) *Multiple Beat*: The terminal node transmits the deceptive packet without setting the recipient field as many times as the *TTL* value. It might be argued that such excessive transmission can rapidly deplete the terminal node's energy. However, we note that a terminal node is a leaf in the network and does not relay as many packets as other nodes. Therefore, a terminal has relatively abundant energy to be used for the benefit of improving the anonymity of the BS.

In *Drop* setting, terminal nodes are not participating in AD approach and are not transmitting any deceptive packets. Such an option is pursued if it is important to preserve the terminals' energy. Meanwhile, the extra deceptive transmissions in the *Single* and *Multiple Beat* variants increase the traffic volume of the network. Being unable to distinguish between the real and deceptive packets, the adversary must intercept, track, and take into account the extra transmissions. Therefore, the extra deceptive transmissions add false evidence and could be disruptive to the adversary's analysis. Furthermore, terminal nodes are located on the network periphery and would give the false perception of a BS in the close-by vicinity or beyond the area boundaries. The latter forces the adversary to expand the monitoring area to account for such possibility and to tradeoff between a lower grid resolution or a higher analysis complexity [16]. Based on the aforementioned reasoning, the *Multiple Beat* is the most ideal choice. In Section VII, we compare the impact of *Single Beat* and *Multiple Beat* from an energy and anonymity points of view to help the network designer in selecting either based on the network's requirement.

C. ILLUSTRATIVE EXAMPLES

In this section we provide three simple examples to show AD in action. Example #1 focus is on AD's behavior in vicinity

of the BS. Example #2 details AD's steps in constructing data packets and setting custom fields in the header. It also explains in detail how each node employs the cover-up selection criteria and routing rules. Example #3 is an elaborate example to show use of AD in directing the deceptive packets away from the BS. It also demonstrates the case in which deceptive packet reaches a terminal node.

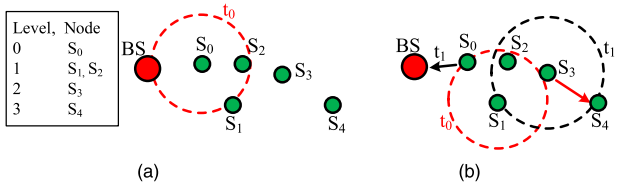

FIGURE 17. Assisted Deception-Examples. a) Trigger node S_0 is a level 0 node. b) Trigger node S_1 is a level 1 node.

Fig. 17(a) depicts Example #1, where S_0 with $level = 0$ is one hop away from the BS. It transmits a data packet at t_0. Since such a packet is not relayed by the BS or any other node, no deceptive transmissions are generated and S_0 does not designate a cover-up node in the data packet header.

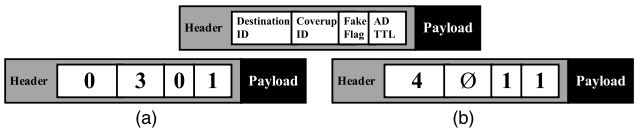

FIGURE 18. AD-R Packets of Example #2. a) Data packet constructed by node#1 b) Deceptive packet constructed by node#3.

In Example #2, shown in Fig. 17(b), S_1 with $level = 1$ transmits its data packet to S_0 at t_0. S_0 relays such a data packet to BS at t_1. S_1 is a trigger node, and needs to specify in its packet which among its three neighbors, S_0, S_2 and S_3, should act as a cover-up. Node S_0 is disqualified as cover-up since its level is less than that of S_1. S_3 is farther from the next hop to the BS, S_0 in this case, than S_2. Thus, S_3 is designated as a cover-up node. The *TTL* is set to 1, which is the level of the data packet source, i.e., S_1. Fig. 18(a) shows the formed data packet. Note that *DestinationID* is a standard field in the packet header and is set to point to S_0 as the next hop on the data route. The transmission of S_1 will be overheard by all its neighbors; S_2 does not find its ID in neither *DestinationID* nor *CoverupID* and therefore does not take any action. The setting of $FakeFlag = 0$ and $DestinationID = 0$ indicates to S_0 that it must route the data packet forward to the next hop, which is the BS in this example. Having $FakeFlag = 0$, and $CoverupID = 3$ tells S_3 that it has been chosen as the cover-up node. As the received packet is a data packet and not a deceptive one, *Rule #2* is not applicable and hence *TTL* value is not reduced upon reception.

As the designated cover-up node, S_3 constructs and sends a deceptive packet at t_1. Node S_3 has only one neighbor that fulfills *Rule #1*, namely, S_4. Fig. 18(b) shows the format of such a deceptive packet. Note that the cover-up field is set to null to ensure that no new cover-up node is picked. Lastly, *FakeFlag* is set to 1 to indicate a deceptive packet type. The deceptive packet transmission by S_3 can be heard by S_1, S_2, and S_4, yet the latter takes action given the *DestinationID* in the header. Since *FakeFlag* is set to 1, S_4 decrements the *TTL* value by 1, which becomes zero in this case, causing S_4 to discard the packet. As shown in Fig. 17(b), only one deceptive packet is generated by S_3 to cover the data transmission of S_0. From an observer's perspective, the paths ($S_1 \rightarrow S_0 \rightarrow BS$) and ($S_1 \rightarrow S_3 \rightarrow S_4$) have the same length and the corresponding nodes make the same number of transmissions; therefore both paths are similarly evaluated by ET and EET, i.e., thanks to AD, the significant of the data path is diminished by the deceptive path.

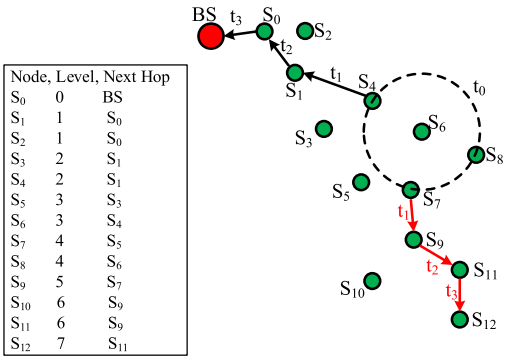

FIGURE 19. Assisted Deception - Example #3.

Example #3, shown in Fig. 19, is more elaborate. At t_0, a trigger node S_6 generates a data packet that is relayed by S_4, S_1, and S_0 at t_2, t_1, and t_0 to reach the BS, respectively. As a trigger node S_6 must pick a cover-up node from the list of its neighbors (S_4, S_7, S_8). S_4 is the next hop of the data packet toward the BS. S_8 is the farthest from S_4 (*Criterion #1*), but at the same time S_6 is its next hop, which dissatisfies *Criterion #2*. Therefore, S_6 is left with S_7 as its only choice for acting as a cover-up node. Fig. 20(a) shows the data packet that S_6 forms with *CoverupID* set to 7 and *TTL* set to S_6's level; 3. S_7 identifies itself as the cover-up for node S_6 when it overhears the data. *Rule 2* applies to deceptive packets, therefore the *TTL* of 3 is not decremented by S_7. S_7 prepares the deceptive packet shown in Fig. 20(b); the packet is destined to S_9, which is the only neighbor of S_7 fulfilling *Rule #1*. Upon receiving $S_7's$ packet, S_9 confirms its role when seeing $DestinationID = 9$, and applies *Rule #2* since *FakeFlag* is set. Hence, *TTL* is decremented by 1 to become equal to 2; given that *TTL* is not zero, S_9 must route the deceptive packet where its two neighbors, S_{10} and S_{11}, fulfill *Rule #1*. AD picks one of those two neighbors randomly. Assuming S_{11} is selected, the deceptive packet in Fig. 20(c) is formed and transmitted by S_9. S_{11} decrements *TTL* ($2 - 1 = 1$) upon reception of the deceptive packet and finds out that S_{12} is the only neighbor fulfilling *Rule #1*. S_{11} then prepares the deceptive packet shown in Fig. 20(d), and transmits it at t_3. When S_{12} receives such transmission,

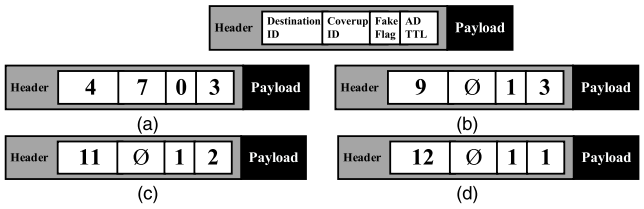

FIGURE 20. AD-R packets of Example #3. a) Data packet constructed by node#6. Deceptive packets constructed by: b) node#7 c) node#9 d) node#11.

it reduces *TTL*; since *TTL* reaches zero, S_{12} does not relay the deceptive packet and drops it. Overall, by tracking and correlating transmissions an adversary can infer that there are two paths, namely, ($S_6 \rightarrow S_4 \rightarrow S_1 \rightarrow S_0 \rightarrow BS$) and ($S_6 \rightarrow S_7 \rightarrow S_9 \rightarrow S_{11} \rightarrow S_{12}$). Both paths have the same length and same number of transmissions and hence will be analyzed similarly by ET/EET, which confirms the effectiveness of AD.

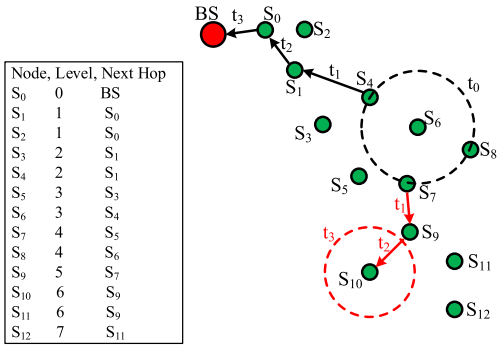

FIGURE 21. Assisted Deception - altered route in Example #3.

In Example #3, S_9 has more than one neighbor fulfilling *Rule #1*. Earlier we assumed that S_{11} is randomly picked as the next hop. Let us now check the outcome if S_{10} is used instead. Fig. 21 and Fig. 22(a) show such an alternative scenario and the corresponding deceptive packet, respectively. At t_2 node S_{10} receives the deceptive packet. It decrements *TTL* which continues to exceed zero, meaning that S_{10} needs to route the deceptive packet. However, as is shown in Fig. 21, S_{10} is a terminal node and has no neighbor to fulfill *Rule #1*. As discussed earlier, AD applies either a *Single Beat* or *Multiple Beat* strategy at terminal nodes. In this example, since *TTL* equals one at S_{10}, *Multiple Beat* acts similar to *Single Beat* and only one deceptive packet is transmitted. S_{10} forms a deceptive packet that is shown in Fig. 22(b) with both *DestinationID* and *CoverupID* are set to null. Upon transmission, none of the reachable neighbors processes such a deceptive packet.

D. APPLICATION ADAPTABILITY

AD is a versatile and flexible countermeasure. Depending on application, nature of threat, and tolerance of overhead, a designer can pick a suitable configuration. This section discusses how two AD parameters can be utilized to determine

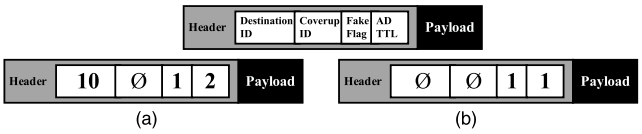

FIGURE 22. AD-R packets of altered route in Example #3. Constructed deceptive packets by: a) node#9 b) node#10.

the level of node engagement to meet multiple application objectives. In Section VII, we show simulation results under different design choices and provide guidelines on effectiveness and overhead trade-off.

1) AGGRESSIVE VS. CONSERVATIVE SETTING

In an event-based network's operation model, e.g., in target tracking applications, the detection of a specific phenomenon or target causes a sensor node to generate a data packet and transmit it to its next hop to be relayed towards the BS. A relay node only forwards incoming packets and does not generate a data packet unless it detects an event as well. AD introduces deceptive transmission into the network to correspond to the dissemination of data packets. Two variants can be noted based on the frequency of fake packet transmissions. The first variant, which what we have discussed so far, is deemed as conservative and is denoted as Con-AD. In Con-AD, only the node that generates a data packet acts as a trigger and designates a cover-up. Therefore, for each packet of a data source, one and only one deceptive packet is generated. Fig. 23(a) shows a simplified example of Con-AD. At t_0, node S_3 generates a data packet to be relayed to the BS via S_2, S_1, and S_0. Con-AD only considers S_3 as a valid trigger node and employs only S_{13} to make a cover-up transmission at t_1 while S_2 is relying the data packet. The second variant pursues a more aggressive approach, where all nodes – both data generators and relay nodes – are considered trigger nodes. In this case, AD transmits deceptive packets to cover up the relay node transmissions as well as the original data generator. Fig. 23(b) shows the same network as Fig. 23(a) with an Aggressive setting of AD (Agg-AD). At t_1 a deceptive packet is sent to cover up transmission of S_2 that is relaying the data of S_3. However, unlike Con-AD, Agg-AD further generates deceptive packets at t_2 and t_3 to cover up transmissions of S_1 and S_0 as well.

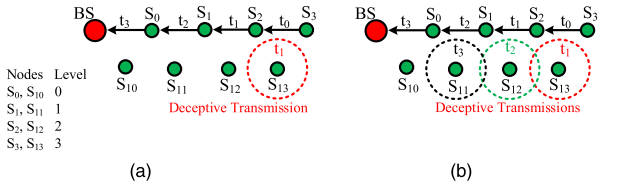

FIGURE 23. a) Conservative Mode of Assisted Deception; Con-AD b) Aggressive Mode of Assisted Deception; Agg-AD.

Obviously, Agg-AD results in generating more deceptive packets compared to Con-AD. Assuming the average path length is q, Agg-AD introduces q times the number of

deceptive packets of Con-AD. The increased cover-up will indeed complicate the adversary's analysis as the number of viable paths becomes 2^q in Agg-AD rather than 2 in the case of Con-AG. However, the overhead also grows significantly. Basically, Agg-AD causes all nodes on the path toward the BS to trigger deceptive packets (S_{11}, S_{12}, S_{13} in Fig. 23(b)) and burdens the lower level sensors as well as high level nodes. Meanwhile, Con-AD engages only one node per data generator (S_{13} in Fig. 23(a)) and hence lowers the load on low level nodes in the network. The application designer has the option to choose between the two variants depending on security requirements versus the network lifetime. In Section VII, we evaluate both configurations and compare the overhead and anonymity gain of each setup. The following lemmas estimate the overhead of Agg-AD when the *Pulse* and *Routing* modes are pursued.

Lemma 1: The overhead of Agg-AD is linearly proportional to the data path length when operating in the *Pulse* mode.

Proof: Assume that q is the average data path length. When operating in the *Pulse* mode, only one fake packet is transmitted as a cover-up. Thus, q deceptive packets are generated and transmitted, corresponding to each node on the data path. If the shortest paths are used for data routing, q can be replaced by the node level ξ.

Lemma 2: The overhead of Agg-AD is quadratic in the node level when AD operates in the *Routing* mode.

Proof: In the *Routing* mode, a fake packet is generated by the cover-up node and is further disseminated away from the BS. The *TTL* setting determines how many times a deceptive packet is relayed in such a case. Since AD sets the *TTL* to the node's level, ξ, the cover-up for a data source X will generate a fake packet that gets relayed ξ times. In Agg-AD every node on the data path from X to the BS, will have a cover-up generated deceptive packet. Thus, assuming that the shortest path is used for routing data, additional relaying activities of ξ-1, ξ-2, ..., 1, will take place corresponding to each node on the data path. Thus, the total number of relaying activities will be $\xi + (\xi\text{-}1) + (\xi\text{-}2) + \ldots + 1$. Recognizing that it is an arithmetic series, the total number of deceptive transmissions becomes $1/2\ \xi(\xi+1)$. Thus, the overhead in terms of transmissions count is quadratic in ξ.

2) ZONING AND RATE SETTING

Examples of #1 and #2 point out an interesting design decision for AD. Nodes at level 0 (one hop from the BS) do not trigger or transmit any deceptive packets, while those at level 1 (two hops from the BS) trigger deceptive packets without transmitting any. On the other hand, Fig. 23 shows that level 1 nodes participate in covering up the relay transmissions at level 0 when Agg-AD is employed instead of Con-AD. Overall, AD is designed to avoid imposing overhead on nodes at level 0. If Con-AD is employed, AD also has zero overhead on level 1 sensors. In a typical WSN network, nodes closer to the BS relay more packets than other nodes and therefore use more energy and have shorter lifespan. AD avoids imposing overhead on these nodes and engages the relatively less-loaded nodes that are farther away from the BS. The network designer can extend AD's default design and instrument Zoning to instruct nodes of a certain level to either participate in AD or not. For example, the designer may decide that any nodes with level less than l should not participate in deceptive packet generation in order to avoid shortening their lifetime.

Published studies like [22], [64]–[66] have shown that injecting a high number of deceptive packets in areas with low traffic density would vary the traffic patterns and boost the anonymity of the BS. Similarly, AD allows fine tuning of the number of deceptive packets that a node in a certain level generates. Thus, the designer can configure a node within specific level to generate more than one deceptive packet when it is chosen as a cover-up. For example, nodes with level l where $l_1 < l < l_2$, could be made to transmit n deceptive packets instead of default value of 1. AD distinguishes itself from other countermeasures by basing the setting the rate of deceptive packet generation on the node level within the network topology, rather than the *Belief* measure of cells. Note also that AD also targets temporal correlation unlike other approaches. By exploiting zone and rate setting, a designer could divide the network to a series of layers and set different rates for each layer. Such flexibility allows deciding which nodes participate in AD and how much burden nodes at each level will have for achieving the best BS anonymity.

VII. SIMULATIONS RESULT

The effectiveness of the EET attack model, and the AD countermeasure is validated through simulation. This section discusses the validation environment, performance metrics, and simulation results.

A. SIMULATION ENVIRONMENT AND EXPERIMENT SETUP

The granularity of our analysis does not require the implementation of all layers of the communication protocol stack. Hence, we have decided to develop our own validation simulation environment in order to expedite the process and have better control on adjusting the relevant parameters. We have developed an event-driven target tracking network simulator in Java. Medium access collisions are ignored in order to capture the performance of countermeasures at the network layer for a true comparison among them. The network consists of 200 nodes that are deployed in a field of $1000 \times 1000\ m^2$ via a uniform random distribution function. Nodes have the same capabilities and report their data via shortest path routing algorithm to a randomly deployed BS within the area. A node generates a data packet only when there is a target in their sensing vicinity. Table 9 shows the relevant node configuration parameters. Communication and energy dissipation models of [67] are used in the simulation and listed in Table 10. All packets are encrypted, and no useful data can be extracted by investigating their headers. Table 11 shows the size of various packet types.

TABLE 9. Sensor parameters.

Sensing Range	*120 m*
Max Transmission Range	*120 m*
Avg Transmission Range	*100m*
Buffer size	*15 packets*
Duty Cycle	*1sec*

TABLE 10. Parameters for the communication energy model.

Energy dissipated in transceiver electronics	*50 nJ/bit*
Energy dissipated in transmitter Amplifier	*100pJ.bit/m2*
Path loss factor	*2*
Data Transmission Bit rate	*2Mbps*

TABLE 11. Packet types and their sizes.

Data packet size	*10Kbits*
Routing packet size	*2Kbits*
Deceptive packet size	*10Kbist*

TABLE 12. Stats on max node level of randomly generated topologies.

Max Node Level	*# of topologies*
8	*3*
9	*7*
10	*5*
11	*11*
12	*7*
13	*10*
14	*6*
15	*0*
16	*1*
Total	*50*

Fifty randomly generated topologies are used in each simulation run. The results are averaged over all topologies. Table 12 shows the number of topologies with each max node level. Targets cross the area with speed, angle of travel and starting points being randomly selected. While comparing countermeasures, the same target pattern is used in order to eliminate variability in the performance measurements due to the data generation profile. A passive adversary intercepts all transmissions of the network. The adversary uses a grid of 10×10, i.e., a total of 100 cells. By using (14) we have $\Delta T = 68.4$ms.

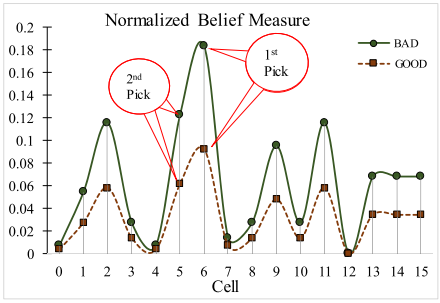

FIGURE 24. GOOD reduces *Belief* measure 50% compared to BAD.

B. METRCIS

Traffic analysis countermeasures often achieve BS anonymity by pursuing inefficient routing topology and/or introducing redundant packet transmissions, which constitute an overhead for the network. In essence the overhead can be gauged based on the extra transmissions compared to the optimal network operation settings. A higher transmission count and longer haul communication increase energy consumption and diminish the network lifespan [15]. Altering routes, imposing packet delay, or introducing extra packets would affect the data delivery latency and impact network throughput [27]. Therefore, energy consumption, and packet delivery delay are suitable metrics for assessing the overhead. Meanwhile, the use of normalized *Belief* is very popular for measuring the BS anonymity. An adversary picks the cell with the highest *Belief* as the BS location. The *Belief* value of the selected cell is not as important, and the *Belief* distribution of all cells is in fact what matters the most. Therefore, comparing countermeasures by their impact on *Belief* might be misleading. To elaborate, let us assume a hypothetical approach called GOOD that reduces the *Belief* of the BS cell by 50% compared to a BAD countermeasure. Even though GOOD seems to be an obvious winner, a closer analysis reveals that GOOD reduces the *Belief* measure of all grid cells by 50%. Fig. 24 highlights such an observation. Even though the *Belief* values are different, the adversary's picks are identical in both approaches, where cell #6 is the first pick and cell #5 is the second pick. In [22], we have introduced standard deviation (STDEV) of normalized *Belief* measure as an indicator of the overall uncertainty that a countermeasure imposes on adversary. A high value of STDEV means that there are cells that significantly deviate from the average. An adversary can easily filter out/in the cells of a grid based on their distinguishability (high value or low value) and implement targeted attack on them; e.g. Zoom strategy [16] or EARS [63]. Thus, a low value of STDEV is the sign of better anonymity. In the rest of this subsection, we introduce three new metrics.

1) SUCCESS RATE

In [64], we introduced Success Rate as a new metric to compare the effectiveness of countermeasures against an in-situ adversary. In a pool of random topologies, it depicts the

number of times an adversary finds the location of BS. An effective countermeasure increases anonymity of the BS and hence decreases the adversary's Success Rate. That makes Success Rate a simple yet interesting metric. Unlike an in-situ adversary, in this work a global adversary that has oversight over the whole area is considered. The main goal of the global adversary is the same as the in-situ one, which is finding the BS. Thus, Success Rate is an applicable metric in both adversary models.

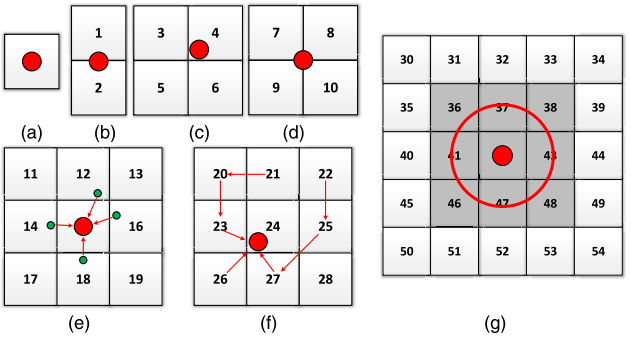

FIGURE 25. Location of BS in respect to cells and Adversary's approach in locating it.

In Section IV, it was established that an adversary uses a grid model to conduct the traffic analysis at the level of cells. The adversary does not have enough insight on the network's topology and the BS location while forming the grid. Hence, the BS might end up (i) at center of a cell, Fig. 25(a), (ii) on the edge of two neighboring cells, Fig. 25(b), (iii) at the corner of a cell, Fig. 25(c), or (iv) at the common corner of 4 neighboring cells, Fig. 25(d). Hence, the BS location in a grid might be tied to one or more cells. Also, the node density or route setup can make the BS to be the only entity in a cell, as illustrated in Fig. 25(e) and Fig. 25(f) respectively. With no other nodes in the cell, no transmission from the cell is recorded. Therefore, identifying the exact BS cell will inherently be subject to inaccuracy. To account for such cases, the adversary considers all cells within a circle to the center of the BS and radius of transmission as the location of BS; Fig. 25(g). If an adversary picks any of the shaded cells shown in Fig. 25(g), it is considered a win and is counted towards its Success Rate.

2) BS RANK

Success Rate is based on a binary criterion; win or lose. An adversary wins if and only if the BS cell has the highest normalized *Belief* measure in the grid; i.e. the first pick and first point of attack. If the BS cell has the second highest value, Success Rate counts that as a loss. In practice, an adversary can launch concurrent or sequential attacks on the n top cells. Therefore, whether the BS cell is amongst the n top cells, impacts its anonymity. If a technique reduces the *Belief* of the BS cell relative to the other grid cells and results in moving it from a high rank (e.g. 2^{nd} place) to a lower rank (e.g. 10^{th} place), it is considered a better countermeasure than the one that does not change the rank. The BS Rank aims to compare countermeasures with respect to their actual effectiveness in concealing the BS cell within the grid. A higher BS Rank means increased detectability and lower anonymity, and vice versa.

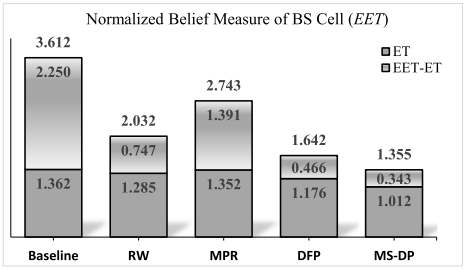

FIGURE 26. Percentage of growth in *Belief* in BS cell contributed by EET relative to ET.

3) SAFE DISTANCE

Countermeasures aim to redirect the focus of the adversary away from the BS cell and towards other cells. The farther the cell that an adversary picks from the actual position of the BS, the safer the BS is. The proximity to the actual BS position is particularly important, if the adversary aims to launch a follow-up physical attack, e.g. by a missile, or radio jamming, once locating the BS. To measure and compare countermeasures based on physically diverting the location of attack farther from the BS, we propose a Safe Distance measure. It is an indicator of the physical proximity between the BS cell and the cell that the adversary has picked. In this work, we measures Safe Distance in terms of the number of cells, i.e., the Safe Distance between two horizontally or vertically neighboring cells is 1, diagonally neighboring cells is $\sqrt{(1^2+1^2)} \approx 1.41$.

C. ET VERSUS EET

EET enhances ET by addition of temporal correlation. The simulation results confirm the strength of EET. In this subsection, results for five network models are presented. The baseline represents a network without any countermeasure in place. The effectiveness of ET and ETT are compared while the following anonymity boosting techniques are employed: Random Walk (RW), Multi-Parent Routing (MPR), and Differential Fractal Propagation (DFP) approaches from [15], and Multiple Destinations-Single Deceptive Packet (MS-DP) model of [22].

Fig. 26 shows normalized *Belief* values of the BS cell while applying EET. The figure also shows the performance gain achieved by switching from EET to ET, denoted as EET-ET. All the bars show that EET improves *Belief* of the BS cell. The highest *Belief* corresponds to the baseline due to the lack of any countermeasure. DFP and MS-DP are the least impacted, which is an indication that they are more effective countermeasures than RW and MPR. Such increased effectiveness comes with higher overhead as seen in Fig. 27,

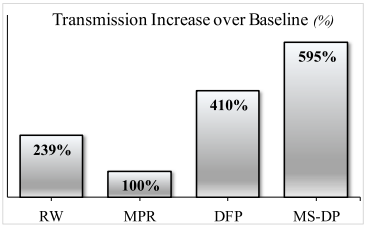

FIGURE 27. Transmission cost of countermeasures.

where both DFP and MS-DP have considerable increase in transmission count, relative to the baseline. RW routes packets randomly until they reach the BS, and thus it increases the number of transmissions by 239%. MPR, on the other hand, uses an optimal route towards the BS and does not increase the number of transmissions. DFP and MS-DP inject deceptive packets in the network to boost anonymity of the BS, therefore, the number of transmissions grows to 410% and 595%, respectively.

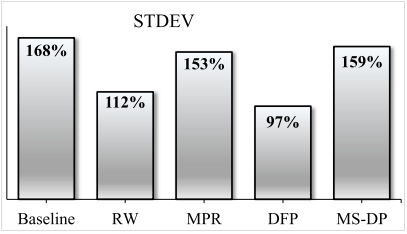

FIGURE 28. STDEV gain by switching from ET to EET.

Fig. 28 shows the change in the STDEV metric once the adversary switches to EET. DFP is showing a slight decrease in STDEV compared to when ET is employed. Other countermeasures experience a jump in STDEV when the adversary uses EET. Fundamentally, a countermeasure aims to make all cells to be possible choices for the adversary. Clearly, EET is better than ET in distinguishing critical and important cells from the rest. The ability of EET in distinguishing important cells is more evident in the Success Rate graph shown in Fig. 29(a). By switching to EET, the adversary's success in accurately finding the BS jumps from 20% to 82% for the baseline. EET also yields 42%, 50%, and 26% increase in Success Rate for RW, MPR, and DFP, respectively. The MS-DP is the countermeasure with the smallest increase in detectability (6%) when EET is employed.

The BS Rank graph is shown in Fig. 29(b). When ET is used, the average BS rank among all 100 cells of the grid is 34 or less for all five network configurations. ETT significantly improves the adversary's detectability by 4.1, 3.6, 3.4, 2.4, and 1.4 times of that of the baseline, RW, MPR, DFP and MS-DP, respectively. In Fig. 29(c) we show the results for the Safe Distance in terms of the number of cells. Clearly, switching to EET makes the adversary's first pick to be in a closer proximity of the BS cell than ET. For example, under RW, the first pick is 1.82 and 3.45 cells away from the BS when EET and ET are used by adversary, respectively.

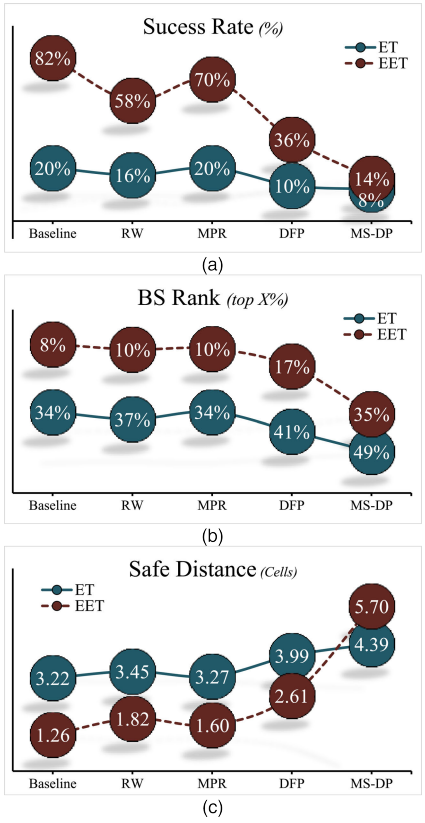

FIGURE 29. ET vs. EET.

Interestingly, MS-DP is showing a reverse effect, where EET results in 5.7 cell distance while ET averages at 4.39 cells. Basically, MS-DP selects cells with low traffic to generate deceptive packets and form routes among them. Thus, the temporal correlation due to transmitting deceptive packets, diverts the adversary's attention to regions farther from the BS. The Safe Distance metric enables us to identify such subtle yet important impact of MS-DP countermeasure.

Both the application designer and the adversary gain a better understanding of the network by combining our newly introduced metrics (Success Rate, Safe Distance, BS Rank, and STDEV) alongside with the *Belief* measure and transmission rate. For example, based on Fig. 26, it might appear that MPR is a decent countermeasure since it reduces the *Belief* measure of the BS cell; yet, Fig. 29(a) reveals that MPR has the same Success Rate as the baseline case if ET is employed. Another example is when comparing DFP and MS-DP in Fig. 26, where both yield almost the same *Belief* value. Hence, the extra transmissions that MS-DP introduces (Fig. 27) do not seem justified. However, when we look at Success Rate in Fig. 29(a) and BS Rank in Fig. 29(b), it is clear that MS-DP is yielding considerable improvements over DFP; especially when the adversary is using EET.

D. ASSISTED DECEPTION

Adding extra fake/deceptive packets is a common approach among many contemporary countermeasures. AD stands out

by timing the deceptive packets in order to counter the temporal correlation of EET. AD also provides a variety of configurable settings (variants) that enables a network designer to fine-tune the performance. In the *default* setting of AD, all nodes participate in AD and we do not specifically vary the deceptive packet generation rate. Unlike such *default* setting, *zoning* restricts node participation based on its level. We also consider Con-AD and Agg-AD, under both *Pulse* (AD-P) and *Routing* (AD-R) modes. In this subsection, we study the performance in the different variants, and then compare AD to other countermeasures while utilizing *Zoning*.

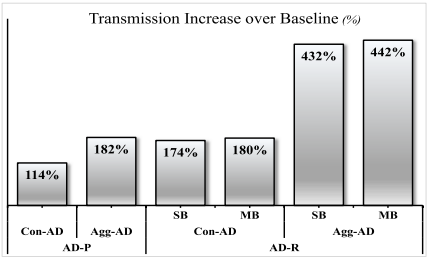

FIGURE 30. Transmission increase of AD flavors over baseline.

Fig. 30 shows the transmission increase for each AD variant over the baseline. When comparing the transmission count, it is clear that Agg-AD imposes high overhead, especially when deceptive packets are routed. i.e., with AD-R. As seen in Fig. 30, a combination of Agg-AD and AD-R grows the transmission rate by over 400%. The difference between the *Single Beat (SB)* and *Multiple Beat (MB)* is not significant since the cases for terminal nodes are not frequently encountered. Fig. 31 shows EET's normalized *Belief* measure value of the BS cell. It also shows how ET is stacked against EET and the achieved gain by switching from ET to EET, denoted as EET-ET. All AD variants are reducing the *Belief* measure regardless of whether ET or EET is used. As expected, the AD variants that have higher transmission rate achieve greater decline in *Belief* measure.

Fig. 32(a) shows the Success Rate for finding the BS. AD is successful in reducing Success Rate for both ET and EET. The default setting of AD, i.e., with both AD-P and Con-AD, is the only configuration which does not impact the EET curve, although it yields a 4% decrease in case of ET. Note that such default configuration has only a moderate increase of 14% in the transmission rate as shown earlier in Fig. 30. For comparison, RW achieves the same result of 4% decrease (Fig. 29(a)) by 139% increase in transmissions (Fig. 27). In other words, AD achieves what RW could achieve, yet at a fraction of the cost. It also should be noted that Agg-AD in the *Multiple Beat (MB)* mode is outperforming the use of Con-AD in the *Routing* mode. That means if the routing overhead is not tolerable by the network, the designer can utilize Agg-AD instead to achieve comparable results (ET curve) or better (EET curve). However, that does not mean that the combination of Con-AD and AD-R should be dismissed;

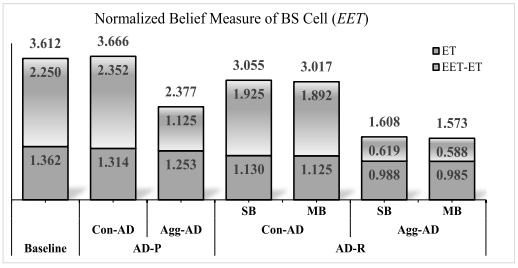

FIGURE 31. Normalized Belief measure of the BS cell when AD is applied.

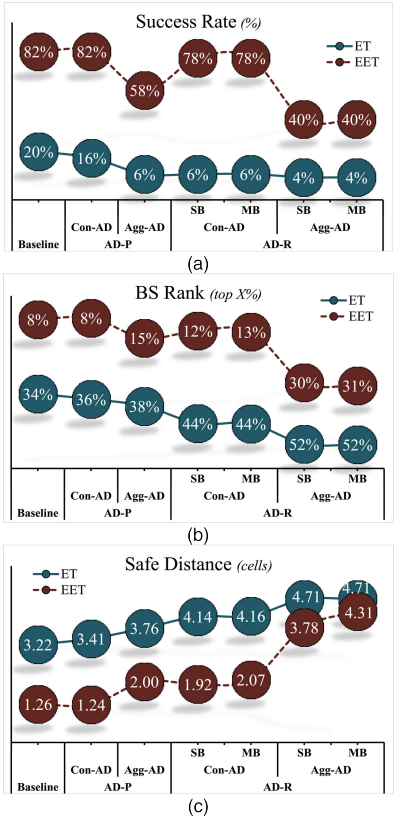

FIGURE 32. AD variants vs. Baseline.

Fig. 32(b) reports the BS Rank and shows that pursuing Con-AD in the *Routing* mode is performing better than Agg-AD in the *Pulse* mode for ET and almost similarly under EET curve.

Fig. 32(a) and Fig. 32(b) demonstrate that *Single Beat (SB)* and *Multiple Beat (MB)* are performing identically. Yet when looking at Fig. 32(c), which shows the Safe Distance metric, it is clear that *MB* version of AD-R is a better option than *SB*. To show the distribution of traffic, Fig. 33 shows the number of transmissions for each node level in the network. The baseline curve shows the expected behavior in which moving away from the BS results in fewer transmissions. The default configuration of AD, i.e., Con-AD operating in *Pulse* mode, follows similar trend and yields a distribution (curve) close to the baseline. However, when switching to Agg-AD, the curve experiences a jump from lower sensor levels

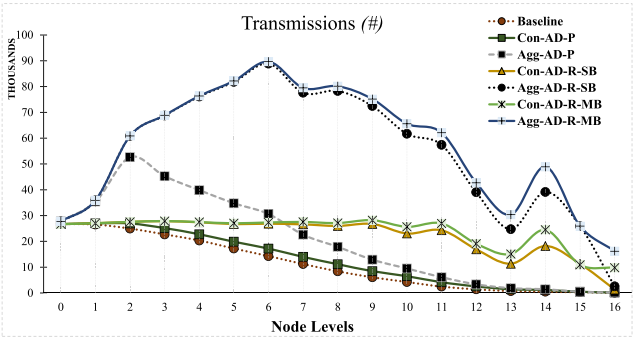

FIGURE 33. Number of transmissions seen in each sensor level after applying AD flavors.

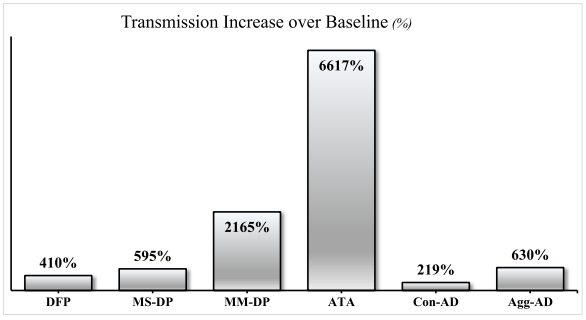

FIGURE 34. Transmission increase over the bassline.

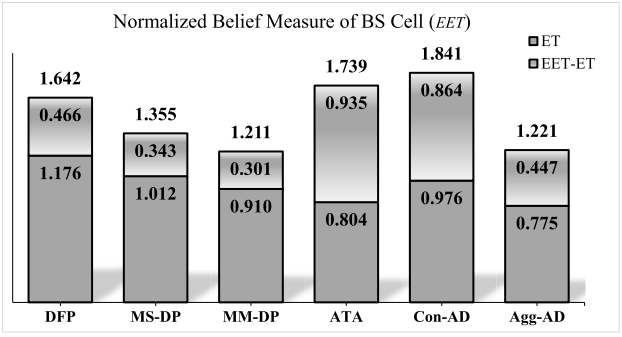

FIGURE 35. Normalized *Belief* measure of BS cell.

and then convergences toward the baseline case. Earlier we noted that Con-AD operating in *Pulse* mode yields a high Success Rate, yet its curve in Fig. 33 reveals that it does not tap into unused energy of distant nodes from the BS. When considering the *Routing* mode, the curves of Con-AD (both *SB* and *MB*) stay almost flat, which is an ideal outcome not only from security point of view but also with respect to network lifetime. We also note the small increase in transmission count for the *Multiple Beat (MB)* relative to the *Single Beat (SB)* for sensor levels of 9 and above. Such an increase implies that the *MB* version uses the energy of higher-level nodes and not the ones that are closer to the BS. As expected, applying Agg-AD in the *Routing* mode increase the transmission rate of nodes at all levels.

To compare the performance of AD against other countermeasures, we use the *Routing* mode which yields the best anonymity results for both the Agg-AD and Con-AD configurations. We used the *Multiple Beat (MB)* when encountering terminal nodes. We used a 4-region zoning model:

$$(0 \le z_1 < \frac{MaxLevel}{4} \le z_2 < \frac{2 \times MaxLevel}{4} \le z_3 < \frac{3 \times MaxLevel}{4} \le z_4 \le \frac{4 \times MaxLevel}{4}),$$

with deceptive packet rates of $\{0, 1, 2, 3\}$ for each zone, respectively. We selected DFP [15], Multiple Destination-Single Packet (MS-DP) and Multiple Destination-Multiple Packets (MM-DP) versions of Deceptive Packets [22], and ATA [25] for comparison. Fig. 34 shows the transmission overhead that each countermeasure imposes on the baseline network. ATA with 6617% increase and DP-MM with 2165% increase are standing out as very costly countermeasures compared to the rest. Fig. 35 shows the normalized *Belief* of the BS cell under EET; it also shows how ET is stacked against EET and the achieved gain when the adversary switches from ET to EET (shown as EET-ET). MM-DP slightly outperforms Agg-AD in countering EET. Yet, Agg-AD wins by far if the ET attack model is used. It is very interesting that ATA does not achieve a good performance, considering its extensive overhead (Fig. 34); the reason lies in its design. Unlike other approaches, ATA does not employ any strategy when generating deceptive packets. It solely relies on brute force to increase the transmission rate of all nodes to the same value. Yet, it yields poor performance compared to the rest of countermeasures. Its weakness is clearer as we show the results for other metrics.

Fig. 36(a) reports the Success Rate of each countermeasure. ATA leads with 2% Success Rate, if an adversary uses ET, followed by MM-DP, Con-AD, and Agg-AD with 4% Success Rate. However, when the adversary uses the superior attack model of EET, ATA is performing similar to Con-AD. Note that Con-AD is achieving the same result with $1/30^{th}$ of the overhead of ATA. Con-AD also defeats DFP in the Success Rate with almost half the transmission overhead (219% vs. 410% as seen in Fig. 34). Similarly, MM-DP is achieving a 6% Success Rate for EET compared to 16% of Agg-AD; such 10% difference is achieved with ∼3.5 times increase in the transmission count (630% vs. 2165% from Fig. 34). A fairer comparison is MS-DP that has almost the same transmission rate as Agg-AD. With Success Rates of 14%(8%) versus 16%(4%) on EET(ET) curves, it is almost a tie between the two. However, the BS Rank metric shown in Fig. 36(b) demonstrates that Agg-AD not only wins over MS-DP, but also outperforms all the other countermeasures including MM-DP.

The Safe Distance results in Fig. 36(c) confirm that AD is more successful than the competing countermeasures in pushing the adversary's prime point of attack farther away from the BS. In Fig. 37, we are showing the number of

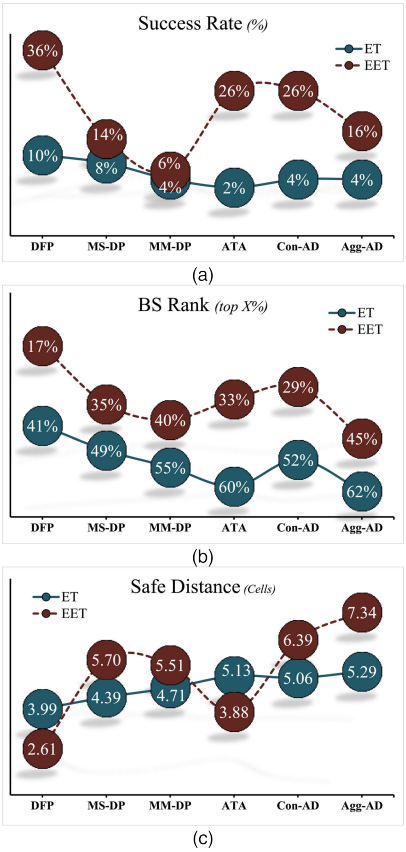

FIGURE 36. AD vs. competition.

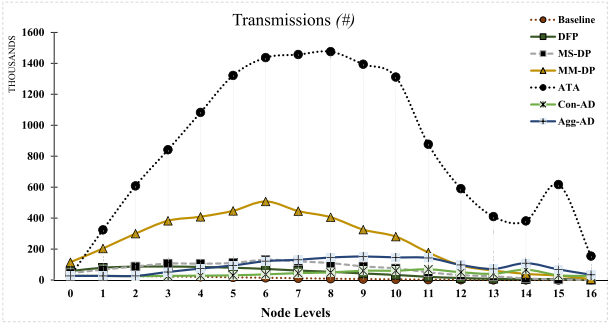

FIGURE 37. Number of transmissions seen in each node level.

transmissions categorized per node level. The high transmission rate of ATA and MM-DP causes them to dominate the plot. It is interesting to note that both approaches are not conscious of the node level and increase the transmission rate for all nodes close and far from the BS. Clearly that could shorten the lifespan of nodes around the BS and could cause a void area that disturbs the network. In Fig. 38 we show the same data of Fig. 37 after eliminating ATA and MM-DP to provide better insight into how the other countermeasures perform. DFP and MS-DP both increase the transmission rate of low-level nodes; such a rate declines as the node level increases. On the other hand, AD shifts the overhead

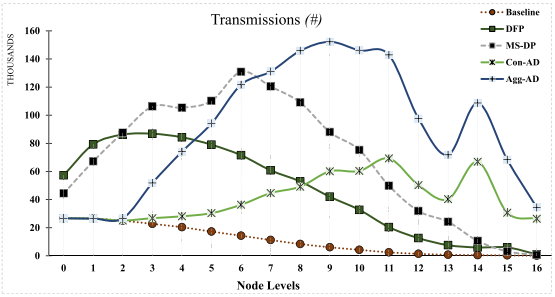

FIGURE 38. Number of transmissions seen in each sensor level (Fig. 37) after removing ATA and MM-DP.

TABLE 13. Acronym Reference.

WSN	Wireless Sensor Networks
BS	Base Station
ET	Evidence Theory
EET	Enhanced Evidence Theory
AD	Assisted Deception
AD-P	Assisted Deception-Pulse mode
AD-R	Assisted Deception-Routing mode
Con-AD	Conservative Assisted Deception
Agg-AD	Aggressive Assisted Deception
RW	Random Walk
MPR	Multi-Parent Routing
DFP	Differential Fractal Propagation
MS-DP	Multiple destinations Single Deceptive Packet
MM-DP	Multiple destinations Multiple Deceptive Packet

to high-level nodes, where there is no impact on nodes in levels 0, 1, 2 thanks to the *zoning* feature of AD.

VIII. CONCLUSION

In a hostile environment, the base-station (BS) is an attractive point of attack considering its critical role in the operation of network. Despite of camouflaging the BS and preventing information leakage from the packet header and payload, an adversary can still intercept radio transmissions and apply traffic analysis to gain knowledge on the topology of the network and locate the BS. ET has been used widely as the adversary's attack model to design countermeasures. In this paper, we have presented an Enhanced ET (EET) model that utilizes the temporal correlation in addition to spatial correlations. To counter EET attack model, we have developed a novel countermeasure called Assisted Deception (AD). AD is a node-aware, distributed, and EET-resilient scheme that coordinates transmission among neighboring nodes to inject deceptive packets in a timely manner. Not only AD prevents the time correlation of data transmissions, it also disturbs the EET analysis and tricks the adversary away from the BS. We have also introduced three new anonymity metrics – Success Rate, BS Rank, Safe Distance – to better gauge the BS anonymity and the impact of countermeasures. The simulations results have shown that current countermeasures could not sustain the anonymity of the BS against an adversary that employs EET. The results have further demonstrated the superiority of AD over other countermeasures. In the future,

we plan to investigate the interplay between traffic analysis and RF fingerprinting and devices robust defense mechanism to protect WSN against the elevated traffic analysis threat.

APPENDIX

See Table 13.

REFERENCES

[1] K. Chopra, K. Gupta, and A. Lambora, "Future Internet: The Internet of Things—A literature review," in *Proc. Int. Conf. Mach. Learn. Big Data, Cloud Parallel Comput. Trends, Prespectives Prospect. Comput.*, Feb. 2019, pp. 135–139.

[2] M. Abdelhafidh, M. Fourati, L. C. Fourati, and A. Chouaya, "Wireless sensor network monitoring system: Architecture, applications and future directions," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 23, no. 4, pp. 413–451, Jan. 2019.

[3] S. Yinbiao and K. Lee, "IEC white paper: Internet of Things: Wireless sensor," Int. Electrotech. Commission, Geneva, Switzerland, White Paper 78, 2014.

[4] J. Jiang, G. Han, H. Wang, and M. Guizani, "A survey on location privacy protection in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 125, pp. 93–114, Jan. 2019.

[5] J. Wang, F. Wang, Z. Cao, F. Lin, and J. Wu, "Sink location privacy protection under direction attack in wireless sensor networks," *Wireless Netw.*, vol. 23, no. 2, pp. 579–591, Feb. 2017.

[6] J. R. Jiang, J. P. Sheu, C. Tu, and J. W. Wu, "An anonymous path routing (APR) protocol for wireless sensor networks," *J. Inf. Sci. Eng.*, vol. 27, no. 2, pp. 657–680, 2011.

[7] J. Kong, X. Hong, and M. Gerla, "An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 8, pp. 888–902, Aug. 2007.

[8] N. Baroutis and M. Younis, "Location privacy in wireless sensor networks," in *Mission-Oriented Sensor Networks and Systems: Art and Science: Foundations*, vol. 1, H. M. Ammari, Ed. Cham, Switzerland: Springer, 2019, pp. 669–714.

[9] Y. Qin, D. Huang, and B. Li, "STARS: A statistical traffic pattern discovery system for MANETs," *IEEE Trans. Dependable Secure Comput.*, vol. 11, no. 2, pp. 181–192, Mar. 2014.

[10] P. Venkitasubramaniam, T. He, L. Tong, and S. Wicker, "Toward an analytical approach to anonymous wireless networking," *IEEE Commun. Mag.*, vol. 46, no. 2, pp. 140–146, Feb. 2008.

[11] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudonymity—A proposal for terminology," in *Designing Privacy Enhancing Technologies* (Lecture Notes in Computer Science), vol. 2009, H. Federrath, Ed. Berlin, Germany: Springer, 2001, pp. 1–9.

[12] D. Huang, "On measuring anonymity for wireless mobile ad-hoc networks," in *Proc. 31st IEEE Conf. Local Comput. Netw.*, vol. 1, Nov. 2006, pp. 779–786.

[13] M. Boulaiche and M. Younis, "Increasing base-station anonymity through illusive void formation," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 25, no. 4, pp. 433–460, 2020.

[14] J. R. Ward and M. Younis, "Cross-layer traffic analysis countermeasures against adaptive attackers of wireless sensor networks," *Wireless Netw.*, vol. 25, no. 5, pp. 2869–2887, Jul. 2019.

[15] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Proc. 1st Int. Conf Secur. Priv. Emerg. Areas Commun. Netw.*, Sep. 2005, pp. 113–126.

[16] Y. Ebrahimi and M. Younis, "Increasing transmission power for higher base-station anonymity in wireless sensor network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2011, pp. 1–5.

[17] S. Alsemairi and M. Younis, "Cross-layer technique for boosting base-station anonymity in wireless sensor networks," *Int. J. Commun. Syst.*, vol. 30, no. 13, p. e3280, Sep. 2017.

[18] N. Baroutis and M. Younis, "Load-conscious maximization of base-station location privacy in wireless sensor networks," *Comput. Netw.*, vol. 124, pp. 126–139, Sep. 2017.

[19] S. Alsemairi and M. Younis, "Forming a cluster-mesh topology to boost base-station anonymity in wireless sensor networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6.

[20] N. Baroutis and M. Younis, "Boosting base-station anonymity in wireless sensor networks through illusive multiple-sink traffic," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–7.

[21] N. Baroutis and M. Younis, "Using fake sinks and deceptive relays to boost base-station anonymity in wireless sensor network," in *Proc. IEEE 40th Conf. Local Comput. Netw. (LCN)*, vols. 26–29, Oct. 2015, pp. 109–116.

[22] Y. Ebrahimi and M. Younis, "Using deceptive packets to increase base-station anonymity in wireless sensor network," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jul. 2011, pp. 842–847.

[23] U. Acharya and M. Younis, "Increasing base-station anonymity in wireless sensor networks," *Ad Hoc Netw.*, vol. 8, no. 8, pp. 791–809, Nov. 2010.

[24] J. Deng, R. Han, and S. Mishra, "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," *Pervas. Mobile Comput.*, vol. 2, no. 2, pp. 159–186, Apr. 2006.

[25] B. Di Ying, D. Makrakis, and H. T. Mouftah, "Anti-traffic analysis attack for location privacy in WSNs," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, pp. 1–15, Dec. 2014.

[26] T. Yan, Y. Bi, L. Sun, and H. Zhu, "Probability based dynamic load-balancing tree algorithm for wireless sensor networks," in *Networking and Mobile Computing* (Lecture Notes in Computer Science), vol. 3619, X. Lu and W. Zhao, Eds. Berlin, Germany: Springer, 2005, pp. 682–691.

[27] Y. Ebrahimi and M. Younis, "Novel assessment metric and countermeasures for traffic attack threats in wireless sensor networks," in *Proc. 37th Annu. IEEE Conf. Local Comput. Netw. (LCN)*, Oct. 2012, pp. 340–343.

[28] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, 2002.

[29] A. Roxin, J. Gaber, M. Wack, and A. Nait-Sidi-Moh, "Survey of wireless geolocation techniques," in *Proc. IEEE Globecom Workshops (GLOBECOM)*, Nov. 2007, pp. 1–9.

[30] N. Patwari, J. N. Ash, S. Kyperountas, A. O. H., R. L. Moses, and N. S. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 54–69, Jul. 2005.

[31] S. Seys and B. Preneel, "ARM: Anonymous routing protocol for mobile ad hoc networks," *Int. J. Wireless Mobile Comput.*, vol. 3, no. 3, pp. 145–155, Oct. 2009.

[32] G. Mao, B. Fidan, and B. D. O. Anderson, "Wireless sensor network localization techniques," *Comput. Netw.*, vol. 51, no. 10, pp. 2529–2553, Jul. 2007.

[33] P. Rong and M. L. Sichitiu, "Angle of arrival localization for wireless sensor networks," in *Proc. 3rd Annu. IEEE Commun. Soc. Sensor Ad Hoc Commun. Netw.*, Sep. 2006, pp. 374–382.

[34] M. Pandey and S. Verma, "Privacy provisioning in wireless sensor networks," *Wireless Pers. Commun.*, vol. 75, no. 2, pp. 1115–1140, Mar. 2014.

[35] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1501–1514, Nov. 2009.

[36] A. Abuladel and O. Bamasag, "Data and location privacy issues in IoT applications," in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Mar. 2020, pp. 1–6.

[37] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," *Sustain. Cities Soc.*, vol. 54, Mar. 2020, Art. no. 101728.

[38] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[39] C.-W. Chen and Y.-R. Tsai, "Location privacy in unattended wireless sensor networks upon the requirement of data survivability," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1480–1490, Aug. 2011.

[40] H. Park, S. Song, B.-Y. Choi, and C.-T. Huang, "PASSAGES: Preserving anonymity of sources and sinks against global eavesdroppers," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 210–214.

[41] H. Wang, G. Han, C. Zhu, S. Chan, and W. Zhang, "TCSLP: A trace cost based source location privacy protection scheme in WSNs for smart cities," *Future Gener. Comput. Syst.*, vol. 107, pp. 965–974, Jun. 2020.

[42] M. F. Al-Mistarihi, I. M. Tanash, F. S. Yaseen, and K. A. Darabkh, "Protecting source location privacy in a clustered wireless sensor networks against local eavesdroppers," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 42–54, Feb. 2020.

[43] B. Chakraborty, S. Verma, and K. P. Singh, "Differentially private location privacy preservation in wireless sensor networks," *Wireless Pers. Commun.*, vol. 104, no. 1, pp. 387–406, Jan. 2019.

[44] S. Gupta and B. Prince, "Preserving privacy of source location using random walk: A survey," in *Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2016, pp. 2047–2051.

[45] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1238–1280, 3rd Quart., 2013.
[46] L. Zhou, Y. Shan, and X. Chen, "An anonymous routing scheme for preserving location privacy in wireless sensor networks," in *Proc. IEEE 3rd Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC)*, Mar. 2019, pp. 262–265.
[47] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.
[48] C. Díaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Privacy Enhancing Technologies* (Lecture Notes in Computer Science), vol. 2482, R. Dingledine and P. Syverson, Eds. Berlin, Germany: Springer, 2003, pp. 54–68.
[49] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Privacy Enhancing Technologies* (Lecture Notes in Computer Science), vol. 2482, R. Dingledine and P. Syverson, Eds. Berlin, Germany: Springer, 2003, pp. 41–53.
[50] W. Conner, T. Abdelzaher, and K. Nahrstedt, "Using data aggregation to prevent traffic analysis in wireless sensor networks," in *Distributed Computing in Sensor Systems* (Lecture Notes in Computer Science), vol. 4026. Berlin, Germany: Springer, 2006, pp. 202–217.
[51] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *Proc. IEEE Int. Conf. Netw. Protocols*, Oct. 2007, pp. 314–323.
[52] R. El-Badry and M. Younis, "Providing location anonymity in a multi-base station wireless sensor network," in *Proc. ICC*, 2012, pp. 157-161.
[53] A. Liu, X. Liu, Z. Tang, L. T. Yang, and Z. Shao, "Preserving smart sink-location privacy with delay guaranteed routing scheme for WSNs," *ACM Trans. Embedded Comput. Syst.*, vol. 16, no. 3, pp. 1–25, Jul. 2017.
[54] V. Kumar, A. Kumar, and M. Singh, "Boosting anonymity in wireless sensor networks," in *Proc. 4th Int. Conf. Signal Process., Comput. Control (ISPCC)*, Sep. 2017, pp. 344–348.
[55] G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, "CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2739–2750, Mar. 2019.
[56] Z. W. Hussien, D. S. Qawasmeh, and M. Shurman, "MSCLP: Multi-sinks cluster-based location privacy protection scheme in WSNs for IoT," in *Proc. 32nd Int. Conf. Microelectron. (ICM)*, Dec. 2020, pp. 1–4.
[57] Y. A. Bangash, L.-F. Zeng, and D. Feng, "MimiBS: Mimicking base-station to provide location privacy protection in wireless sensor networks," *J. Comput. Sci. Technol.*, vol. 32, no. 5, pp. 991–1007, Sep. 2017.
[58] I. T. Almalkawi, J. Raed, N. Alghaeb, and M. G. Zapata, "An efficient location privacy scheme for wireless multimedia sensor networks," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2019, pp. 1615–1618.
[59] B. Chakraborty, S. Verma, and K. P. Singh, "Temporal differential privacy in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 155, Apr. 2020, Art. no. 102548.
[60] J. Chen, Z. Lin, Y. Liu, Y. Hu, and X. Du, "Sink location protection protocols based on packet sending rate adjustment," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 1, Jan. 2016, Art. no. 6354514.
[61] V. P. V. Gottumukkala, V. Pandit, H. Li, and D. P. Agrawal, "Base-station location anonymity and security technique (BLAST) for wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 6705–6709.
[62] K. Bicakci, I. E. Bagci, and B. Tavli, "Lifetime bounds of wireless sensor networks preserving perfect sink unobservability," *IEEE Commun. Lett.*, vol. 15, no. 2, pp. 205–207, Feb. 2011.
[63] N. Baroutis and M. Younis, "A novel traffic analysis attack model and base-station anonymity metrics for wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5892–5907, Dec. 2016.
[64] Y. Ebrahimi and M. Younis, "Averting *in-situ* adversaries in wireless sensor network using deceptive traffic," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–5.
[65] X. Li, X. Wang, N. Zheng, Z. Wan, and M. Gu, "Enhanced location privacy protection of base station in wireless sensor networks," in *Proc. 5th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN)*, 2009, pp. 457–464.
[66] P. Priyadarshini and M. Pandey, "Concealing of the base station's location for preserving privacy in wireless sensor network by mitigating traffic patterns," in *Proc. IEEE Int. Conf. Adv. Commun., Control Comput. Technol.*, no. 978, May 2014, pp. 852–857.
[67] W. R. Heinzelman, A. Sinha, A. Wang, and A. P. Chandrakasan, "Energy-scalable algorithms and protocols for wireless microsensor networks," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, vol. 6, Jun. 2000, pp. 3722–3725.

YOUSEF EBRAHIMI received the B.S. degree in computer engineering from the Isfahan University of Technology, Iran, and the M.S. degree in computer engineering from the Sharif University of Technology, Iran. He is currently pursuing the Ph.D. degree in computer engineering with the University of Maryland Baltimore County. He is also an Engineering Manager with Cisco Systems Inc. leading a team of engineers in identifying and addressing escalated problems with network security devices. His research interest includes traffic analysis in IoT and WSN with focus on location anonymity.

MOHAMED YOUNIS (Senior Member, IEEE) received the Ph.D. degree in computer science from the New Jersey Institute of Technology, Newark, NJ, USA. He is currently a Professor with the Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County (UMBC). Before joining UMBC, he was with the Advanced Systems Technology Group, an Aerospace Electronic Systems Research and Development Organization of Honeywell International Inc. While at Honeywell he led multiple projects for building integrated fault tolerant avionics and dependable computing infrastructure. He also participated in the development of the Redundancy Management System, which is a key component of the Vehicle and Mission Computer for NASA's X-33 space launch vehicle. He has six granted and two pending patents. He has published about 300 technical papers in refereed conferences and journals. His research interests include network architectures and protocols, wireless sensor networks, embedded systems, fault tolerant computing, secure communication, and distributed real-time systems. He is a Senior Member of the IEEE Communications Society. He serves/served on the editorial board of multiple journals and the organizing and technical program committees of numerous conferences.