This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2600585, IEEE Transactions on Smart Grid

Intrusion Detection and Prevention for ZigBee-Based Home Area Networks in Smart Grids

Paria Jokar, *Member, IEEE,* and Victor C.M. Leung, *Fellow, IEEE*

***Abstract*—In this paper we present a novel intrusion detection and prevention system for ZigBee-based home area networks in smart grids, HANIDPS. HANIDPS employs a model-based intrusion detection mechanism as well as a machine learning-based intrusion prevention system to protect the network against a wide range of attack types. The detection module extracts network features and analyzes them to decide whether the network is in a normal state. We use SEP 2.0 specification as well as IEEE 802.15.4 standard to precisely characterize the expected normal behavior. A set of defensive actions are defined for the prevention system which are effective in stopping various attack types. HANIDPS uses Q-learning and through interactions with environment learns the best strategy against an attack. Use of model based approach for intrusion detection and dynamic learning for intrusion prevention, as well as employment of effective mechanisms to stop the attacks, provide a high performance for HANIDPS without the need for prior knowledge of the attacks. Soundness of the proposed method is evaluated through extensive analysis and experiments.**

List of abbreviations

AMI	Advanced metering infrastructure
D	Datagram
EMS	Energy management system
FPR	False positive rate
HAN	Home area network
NAN	Neighborhood area network
NA	Node availability
SN	Sequence number
TR	Traffic rate
HTTPS	Hyper text transfer protocol with secure socket
TCP	Transmission control protocol
U.S.	United States
AM	Air monitor
AGC	Automatic generation control
BIDS	Behavior-rule based IDS
BER	Bit error rate
CSMA-CA	Carrier sense multiple access/collision avoidance
C-IDPS	Central IDPS
DoS	Denial of service
ED	Energy detection
FDI	False data injection
GTS	Guaranteed time slot
IDPS	Intrusion detection and prevention system
IDS	Intrusion detection system
LQI	Link quality indicator
LUT	Look up table
MAC	Medium access control
NIST	National institute of standards and technology
PER	Packet error rate
PHY	Physical
RSS	Received signal strength
ROC	Receiver operating characteristic
SEP 2.0	Smart energy profile 2.0
SDC	Summation of detailed coefficients
SCADA	Supervisory control and data acquisition
SVM	Support vector machine

I. Introduction

From the advent of the smart grid concept, security has always been a major concern. The need for developing intrusion detection systems (IDSs) tailored for smart grid subsystems was emphasized in the United States (U.S.) national institute of standards and technology (NIST) guidelines for smart grid cyber security [1]. Home area networks (HANs) are subsystems within the smart grid which provide the communication among the smart meters and home devices. The dominant HAN technology in North America and many other countries is ZigBee. Being located in insecure environment and use of wireless technology make HANs vulnerable to cyber attacks [2],[3]; this necessitates application of appropriate IDSs. At the same time, since HANs are located in areas far from the utility, receiving the IDS alarms and acting upon them introduces a large operational cost and delay in stopping the attacks. In traditional IDSs, once an attack is detected, an alarm is sent to a network operator who is responsible for finding the roots of the attack and triggering response operations varying from remote diagnosis to on-site inspection. Considering the large scale of smart grids, when human response is expected, a small percentage of false alarms results in a high operational cost. Therefore, intrusion prevention mechanisms which not only detect but also stop the attacks are highly preferable.

In this work we present a novel intrusion detection and prevention system (IDPS) for ZigBee-based HANs, HANIDPS. We use smart energy profile 2.0 (SEP 2.0) protocol specification [4] as well as IEEE 802.15.4 standard (which defines the physical (PHY) and medium access control (MAC) layers of ZigBee), to define a thorough feature space. HANIDPS employs a model-based detection module and a machine learning-based prevention module which dynamically learns the best strategy against an attacker. Through analysis and experiments we show that HANIDPS is able to detect and stop various attack types with a high performance. The main contributions of this work are:

- To the best of our knowledge we are the first who address the problem of automatic intrusion prevention in ZigBee-based HANs. Considering that in HANIDPS the prevention operation is performed automatically, the costs of false positives are low and limited to some network overhead. Also the delay in stopping the attacks is significantly shortened compared to when human intervention is required. This reduces the damages caused by possible attacks.
- HANIDPS is a novel algorithm which utilizes a model-

based IDS along with a dynamic machine learning-based prevention technique to detect and prevent intrusions with low false positive rate (FPR) and without prior knowledge of attacks.

- We introduce a novel high performance spoofing prevention technique as an important defense mechanism in HANIDPS which enables prevention against a variety of attack types. The algorithm is also effective in securing other static wireless sensor networks.

This work is an extension to our previous papers [5]-[7]. In [5], we studied the HAN architecture and IDS requirements for HANs. We compared different intrusion detection methods and suggested application of specification based approach. Accordingly we proposed a specification based IDS for HANs in which the feature space was defined based on the network specifications extracted from the IEEE 802.15.4 standard. In [6] we presented an algorithm for detecting spoofing attacks against static IEEE 802.15.4 networks which works by analyzing the received signal strength (RSS) of network packets. We also introduced an RSS-based spoofing prevention mechanism for ZigBee-based HANs in [7]. This work has several new contributions compared to our previous papers. While [5] only targeted the area of intrusion detection, here we introduce an algorithm which not only is able to detect various attack types but also can automatically stop them. For the detection module we use a model based approach which is a combination of anomaly-based and specification-based IDSs. While in [5] we only used IEEE 802.15.4 standard and common features of wireless networks for defining the feature space, here we also use SEP 2.0 protocol specification. Therefore, the definition of feature space in this work is much more precise compared to [5]. Here, the detection module analyzes 6 features of network traffic, one of them is RSS which is examined using the method we introduced in [6]. In the present work, we define several preventive actions for HANIDPS and design a machine learning based method for choosing the best sequence of actions against an attacker. One of these actions is the spoofing prevention algorithm we introduced in [7]. Therefore, while the methods introduced in [6] and [7] were only designed to detect and stop spoofing attacks, the proposed method in this work is able to detect and stop various attack types without having any previous knowledge about them. The machine learning based prevention method designed in this paper which dynamically learns the best strategy against an attacker is completely new.

The rest of this paper is organized as follows. We survey the related work in Section II and provide an overview of HAN security threats in Section III. Architecture and algorithm of HANIDPS is explained in Section IV. Section V and VI present the theoretical analysis and experimental evaluations of HANIDPS. In Section VII we provide a discussion on performance of HANIDPS against evasion techniques and Section VIII concludes the paper.

II. Related Work

Designing IDSs tailored for smart grid subsystems has attracted the attention of researchers over the last few years. Mitchell et al. [8] introduced a behavior-rule based IDS (BIDS) for securing head ends, distribution access points and smart meters. For each section a set of high-level behavior rules were defined. An intrusion was detected when the behavior rules were violated. This method provides a high accuracy; yet since the behavior rules are high level it is subject to detection delay. Besides, it does not provide an insight into the cause of misbehaviors. A hierarchical distributed IDS for advanced metering infrastructure (AMI) was proposed in [9]. The distributed IDS components were connected through a wireless mesh network. Each component employed support vector machine (SVM) and immune system for detecting intrusions. Applying the same solution for different AMI networks including HANs, NANs and head ends which use different protocols and have different traffic features makes this method inefficient. Unlike [8] and [9] which use the same mechanism for intrusion detection for various AMI networks, we focus on HANs. This enables us to provide a high performance mechanism with the ability of both detecting and preventing the attacks. Authors of [10] and [11] targeted detection of false data injection (FDI) attacks in smart grids. Lo et. al [10], proposed a hybrid IDS framework for AMI which uses power information and sensor placement to detect FDIs. Chen et. al [11], exploited spatial-temporal correlations between grid components for real-time detection of FDIs. A distributed IDS tailored for wireless mesh networks employed in NANs, was proposed in [12]. This work specifically targeted network layer attacks. In [13] a specification-based IDS for communications between smart meters and data aggregators was presented. Using C12.12 standard protocol a set of constrains were made and attacks were detected by monitoring the violations of the security policy. Authors of [14] introduced a two-tier IDS for automatic generation control (AGC) in smart grids. The first tier was a short-term adaptive predictor for system variables, and the second tier performed state inspection to investigate the presence of anomalies. Combination of the two tiers provided a balance between accuracy and real-time requirements of IDS for AGC. We on the other hand focus on HAN protocols and provide a solution for not only detecting but also preventing the attacks. Model-based IDS for intrusion detection in wireless sensor networks has attracted the attention of researchers in the past [15]-[17]. When the number of applications and protocols are limited, model-based IDSs are very effective, since they provide a low FPR and are capable of detecting new attacks. In [15] and [16] model-based IDSs for modbus networks in supervisory control and data acquisition (SCADA) were presented. Ioannis et al. [17] introduced a specification-based IDS for detecting network layer attacks in wireless sensor networks including blackholes and grayholes. HANIDPS also uses a model-based approach. However, it distinguishes itself from [15]-[17] by covering the unique requirements of the area. First, HAN is a stationary network which eliminates the need for monitoring moving objects. Second, HAN coverage area is comparably small and most communications are single hop. Therefore, unlike most IDS solutions for wireless sensor networks which are tailored for network layer protocols our focus is on PHY and MAC layers. Third, none of [15]-[17] addressed the problem of intrusion prevention for a wide range of attack types.

III. HAN Security Threats

Threats against AMI can be viewed in three different ways: by type of attacker, motivation and attack technique. In [18] a threat model for AMI was provided which lists the types of attackers and their motivations as follows:

- Curious eavesdroppers, who are motivated to learn about the activity of their neighbors by listening to the traffic of the surrounding meters or HAN.
- Motivated eavesdroppers, who desire to gather information about potential victims as part of an organized theft.
- Overly intrusive meter data management agencies, which are motivated to gain high-resolution energy and behavior profiles about their users, which can compromise customer privacy. This type of attacker also includes employees who could attempt to spy illegitimately on customers.
- Unethical customers, who are motivated to steal electricity by tampering with the metering system installed inside their homes or to gain control of the devices which should be under control of the utility.
- Active attackers, who are motivated by financial gain or terrorist goals. The objective of a terrorist would be to create large-scale disruption of the grid, either by remotely cutting off many customers or by creating instability in the distribution or transmission networks. Active attackers attracted by financial gain could also use disruptive actions, such as denial of service (DoS) attacks.
- Publicity seekers, who use techniques similar to those of other types of attackers, but in a potentially less harmful way, because they are more interested in fame and usually have limited financial resources.

From the above list unethical customers, active attackers and publicity seekers require to perform active attacks to achieve their goals. Curious and motivated eavesdroppers might perform active or passive eavesdropping. IDSs are effective in protecting the network against active attacks. Overly intrusive meter data management agencies use the data available in head ends rather than targeting the HAN; therefore, are outside the scope of this work.

Smart grid is a new concept. A thorough threat model which provides details on possible attack scenarios and techniques, for different AMI networks and devices, is not available yet; providing such models is an open research topic. Few works have been done in this area over the past few years. In [19] a model for security analysis of smart meters was provided. The authors proposed a systematic method for modeling functionalities of smart meters and deriving attacks that can be mounted on them. McLaughlin et al. [20] conducted a multi-vendor penetration testing on AMI devices within NANs. They developed archetypal attack trees for three classes of attacks: energy fraud, denial of service and targeted disconnect. Grochocki et al. [21] surveyed various threats facing AMI and common attack techniques used to realize them; however, authors of [21] mentioned that methods of compromising HANs are beyond the scope of their work. While a thorough threat model for HANs does not exist in literature yet, and defining one is a stand alone research topic which is beyond the scope of this work, in the following we provide some examples of possible attacks against ZigBee HANs. We also explore a number of representative case studies to connect attacker objectives with individual attack steps. Table I shows a summary of attacks against AMI, based on the threat model provided in [21]. These attacks are applicable for HANs. For detail explanation of each attack we refer the readers to [21].

TABLE I: Example of attacks against ZigBee HANs

Category	Attack technique	Target
DoS	Collision in packet transmission	HAN link layer
DoS	Jamming	HAN physical layer
DoS	Resource exhaustion	Node in HAN
DoS	Destroy node	Node in HAN
Spoofing	Impersonate regular node	Node in HAN
Spoofing	Impersonate master node	Node in HAN
Spoofing	Man-in-the-middle	HAN traffic
Spoofing	Brute-force	Node in HAN
Eavesdropping	Passively listen to traffic	HAN traffic
Eavesdropping	Active cryptanalysis	HAN traffic
Physical	Compromise meter	Node in HAN

A. Case Studies

1) Illegitimate remote turn-on/off commands: This attack can be used by unethical customers, publicity seekers and active attackers with different motivations. An unethical customer might aim to gain control of a specific device which according to the customer utility agreement is under control of the utility. An antisocial publicity seeker might use this attack to achieve fame or unsettle a customer. An active attacker with malicious intentions such as committing theft, kidnapping, etc. can use this attack to distract the customers. Terrorists might use this attack in large scale to cause horror and chaos, or to affect the load curve in order to damage the power system equipment. As a case in point, the attacker sends turn-off messages to all controllable customer equipment. After passing a long enough time which guarantees that the equipment would turn on when allowed, the attacker sends turn-on permission messages. When applied in large scale, the attack results in a sudden increase in the load, which can affect the bulk electric grid. Considering that for performing this attack against HANs the attacker must be within the ZigBee communication range, conducting it in large scale is expensive. But terrorists can be very motivated and have high funding. This attack can be done using the following steps.

- The attacker passively eavesdrops the network traffic or perform active network scanning to learn the link layer address of the authoritative node like energy management system (EMS) and the victim node.
- The attacker needs to learn the authentication credentials of the authoritative node (if authentication is supported); this information can be obtained using brute-force attack.
- The attacker needs to know the encryption key to encrypt the control commands (if encryption is supported). Cryptanalysis techniques can be used for this purpose. Man-in-the-middle attacks might also be helpful in bypassing the encryption system.

- The attacker conducts DoS against the authoritative node to stop it from sending legitimate control commands.
- The attacker impersonates ID of the authoritative node and sends turn-on/off commands on its behalf to the victim node.

2) Stealing customer information: The motivation of this attack is to collect customer information and learn about customer behavior. For instance, in an organized theft an adversary can benefit from knowing the total electricity usage of the household to infer whether the customers are at home or not. The EMS is allowed to request this information from the smart meter, and the smart meter sends the information to EMS through encrypted messages. Considering that HAN traffic may be encrypted and authentication might be required for a node to access the network, this attack may involve the following steps.

- The attacker passively eavesdrops the network traffic or perform active network scanning to learn the link layer address of the EMS.
- The attacker needs to learn the authentication credentials of EMS (if authentication is supported); this information can be obtained using brute-force attack.
- The attacker needs to know the encryption key to encrypt/decrypt the massages (if encryption is supported). Cryptanalysis techniques can be used for this purpose.
- The attacker impersonates ID of the EMS and requests for the usage information.
- The attacker decrypts the messages and collects the message contents.

3) Denial of service against network nodes: An unethical customer may conduct DoS against HAN nodes with the purpose of gaining control of a specific device. By conducting DoS against authoritative nodes or a sensor node on a specific device such as thermostat, customer intervenes with the control commands by the utility and does not allow the utility to control the device. In Section VI-A we introduce several inexpensive DoS techniques against IEEE 802.15.4 networks.

IV. HANIDPS

A. Architecture

HANIDPS is designed for PHY and MAC layers of ZigBee HANs and has two modules, detection and prevention.

1) Detection module: Network traffic between the smart meter and sensor nodes as well as nodes' behavior are monitored, and network features are extracted. These features are analyzed and compared with the expected normal behavior based on the system specification. If one or more of the features are not normal, an intrusion will be detected and the prevention module will be triggered. The detection module uses a combination of anomaly based approach and specification based approach for attack detection which enables it to detect various attack types with high performance. A thorough comparison between different types of IDSs and a discussion on the suitable IDS method for HAN was provided in our previous paper [5]. Specification based IDSs provide a low FPR and have the potential to provide a high detection rate. The strength of this type of IDS depends on the thoroughness of the feature space. HANIDPS uses a combination of anomaly based approach and specification based approach to define a thorough feature space which enables it to detect various attack types with low FPR and high DR. For further information on comparison among different intrusion detection techniques and suitability of each approach for HAN we refer the readers to our previous work [5].

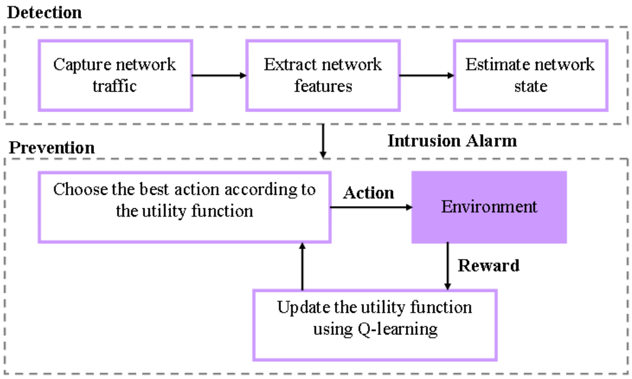

Fig. 1: Block diagram of modules of HANIDPS.

2) Prevention module: Upon receiving an intrusion alarm an action or a set of actions are automatically performed to stop or mitigate a possible attack. HANIDPS preventive actions include spoofing prevention, interference avoidance and dropping malicious packets. An adversary might use various attack types to disturb the network operation. Therefore, appropriate actions are required to countermeasure different attack scenarios. HANIDPS uses reinforcement learning to find the best strategy against an attacker. In reinforcement learning, the process of learning happens via trial and error. Through feedbacks received from the environment, HANIDPS learns what the best and most effective actions are. A block diagram of HANIDPS is shown in Fig. 1.

HANIDPS has two components, monitoring agents and central IDPS (C-IDPS). Agents are installed on sensor nodes and are responsible for monitoring the behavior of the corresponding nodes. They count the packet error rate (PER) and keep a record of RSS values of received frames. Agents send measured PERs to C-IDPS periodically through health messages. Once an attack is detected by C-IDPS, agents might also take part in prevention operations based on the recorded RSS values. Network traffic between sensor nodes flow through C-IDPS. C-IDPS is responsible for extracting and analyzing the network features and health messages to infer the state of the network nodes. Once an abnormal state is detected C-IDPS performs a dynamic defense mechanism in which through Q-learning a set of preventive actions are selected and performed.

Considering that most of the detection and prevention operations are performed by C-IDPS, in order for the HANIDPS to function correctly C-IDPS must be trusted. Therefore, it must be implemented in a highly secure tamper resistant super-node. C-IDPS analyzes the health messages received from the agents to decide whether or not the nodes are available and their PER is in the expected range. Attacks against network nodes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2600585, IEEE Transactions on Smart Grid

(which affect the agents installed on them) that stop them from sending normal traffic, such as DoS attacks, do not affect the operation of HANIDPS; since in this case health messages are not received by C-IDPS and the attack is detected. On the other hand, if a node is penetrated and the attacker sends false data from the node for instance false health messages, intrusion to that node might not be detected, yet it does not affect the operation of HANIDPS for other network nodes.

In the following subsections, we explain the feature space, preventive actions and decision making process to choose the best sequence of actions.

B. Feature Space

The ZigBee alliance, HomeGrid Forum, HomePlug alliance and WiFi alliance created a consortium for interoperability of energy management devices in HANs. The goal was to define the interfaces and messages among smart appliances, smart meters and utilities. The alliances published a draft for smart grid application communication, SEP 2.0. NIST selected SEP 2.0 as a standard profile for smart energy management in home devices. We used this document as well as IEEE 802.15.4 protocol specification and common features of wireless networks to extract network specifications used in defining the feature space for HANIDPS.

The features are selected based on a study of the effect and behavior of several existing attacks against wireless networks, and therefore enable the HANIDPS to detect various attack types. Other features can be added to HANIDPS once new attacks are introduced which affect other aspect of the systems or network. While defining an extensive feature space can potentially enable the IDPS to detect diverse attack types redundant features which only introduce system overhead and delay in the process of attack detection and prevention must be avoided. Components of the feature space are as follows:

f_1) Datagram (D): PHY and MAC layer frame structures according to IEEE 802.15.4 specification are defined for C-IDPS. C-IDPS compares some features of frames like frame size and reserved bits with the standard structure and decides whether the packets are normal. Also according to SEP 2.0, the application layer protocol for home devices is Hyper Text Transfer Protocol with Secure Socket (HTTPS) over Transmission Control Protocol (TCP). The minimum and maximum length for each message, as well as the mandatory and optional fields are defined in the protocol. Therefore, the theoretical minimum and maximum length of packets can be calculated. The total length of a legitimate SEP 2.0 messages is between 508 and 1524 bytes.

f_2) Traffic Rate (TR): SEP 2.0 states that ”to prevent overwhelming network resources, notifications should be sent to a given client for a given resource no more than once every 30 seconds. Notifications for conditional subscriptions should only be sent once within this time period for a given client for a given resource and any additional notifications should not be queued. All devices need to be considerate of network resources”. While in SEP 2.0 end devices are responsible for pulling network time from the network controller, it has been mentioned that the granularity of the devices must be one second. Therefore, a genuine node that complies with the protocol specifications does not surpass a limit for traffic rate.

TABLE II: HAN requirements

Smart Grid Functionality	Bandwidth, Latency, Availability
Advanced Metering Interface	100 kbps/node, 2-15 sec, 99-99.99%
Demand Response	100 kbps/node, 0.5-2 sec, 99-99.99%
Distributed Energy Resources	100 kbps/node, 0.02-15 sec, 99-99.99%
Electric Vehicles	100 kbps/vehicle, 2 sec-5 min, 99-99.99%

f_3) RSS: According to the laws of physics signal strength at a receiver antenna is proportional to the spatial distance between the receiver and the sender. Beside distance, RSS depends on the features of the wireless environment, such as absorption and multipath effect, which makes it hard to predict the power level of frames collected by a receiver. Thus, an attacker cannot simply adjust his power level to match the RSS of a legitimate node. This feature is useful in detecting spoofing attacks in which an adversary masquerades identity of a legitimate node and send traffic on its behalf. Spoofing is a basis for several attacks. In [6] we have introduced a high performance RSS-based method for detecting spoofing attacks in static IEEE 802.15.4 networks. The RSS values of the frames are extracted by air monitors (AMs). The algorithm employs two features of RSS streams, summation of detailed coefficients (SDC) in discrete Haar wavelet transform of the RSS streams and the ratio of out-of-bound frames. Unlike other existing methods, we showed that using both frequency and magnitude features the proposed algorithm provides a high detection performance even when only one AM is used. We use the same algorithm in HANIDPS to decide whether the RSS values are normal or suspicious. For more details on the algorithm we refer the readers to [6].

f_4) Sequence Number (SN): The regular ordering of sequence numbers according to the standard is defined for C-IDPS. Unusual sequence numbers can be suspicious.

f_5) Packet Error Rate (PER): A major cause of high PER is the use of a busy channel. IEEE 802.15.4 employs carrier sense multiple access/collision avoidance (CSMA-CA) to evaluate availability of the channel. Under normal condition PER must be low. However, illegitimate (such as jamming sources) or legal (such as WiFi interference) coexistence of other signals can increase the PER. This will affect the network throughput and cause latency in packet delivery. We use a mathematical model for ZigBee performance to find the acceptable PER which allows the required bandwidth and latency for HAN operations. A summary of network requirements for HAN, as indicated by the U.S. department of energy [22], is provided in Table II. In [23], a model for computing maximum delay and upper bound on data rate in beacon-enabled guaranteed time slot (GTS) Zigbee networks was provided as in (1) and (2).

$$D_{max} = \frac{b}{C} + (k-1) \times BI - (T_{GTS} + T_R) - k \times T_{GTS} \quad (1)$$

$$B_{C,T}(t) = C \times T_{GTS} + C \times (t - (2 \times BI - T_R)) \quad (2)$$

where D_{max} is the maximum delay, b is the minimum burst size, C is the service rate which for ZigBee is 250 kbps,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2600585, IEEE Transactions on Smart Grid

k is the number of GTS slots, BI is the beacon interval, T_{GTS} is the duration of data transmission within the GTS slot, T_R is the portion of the GTS during which there is no data transmission, and $B_{C,T}(t)$ represents the upper bound on data rate. To account for network interference, and considering that the number of re-transmissions before declaring channel access failure in ZigBee specification is 5, [23] modified (1) and (2) by replacing C with C_{adj} as in (3):

$$C_{adj} = P \times C \times \sum_{i=0}^{4} (1-P)^i \tag{3}$$

where P is the probability of a clear channel. As (1), (2) and (3) suggest the maximum delay and guaranteed data rate of a client is a function of the number of assigned GTSs and the probability of clear channel for the client. We calculate the minimum probability of clear channel for different numbers of assigned GTSs, which allows the required performance according to Table II. PER for an IEEE 802.15.4 network in presence of interference is formulated as follows [24]:

$$PER = 1 - (1-P_b)^{N_z - \left[\frac{T_c}{b}\right]} \times \left(1 - P_I^b\right)^{\left[\frac{T_c}{b}\right]} \tag{4}$$

P_b is bit error rate (BER) without interference, P_I^b is BER with interference, N_z is the number of bits in a packet, b is the duration of bit transmission, and T_c is the collision time. Without interference $P = 1 - P_b$ and in presence of interference $P = 1 - P_I^b$. Therefore, we can calculate the threshold for acceptable PER. For instance, using (1), (2) and (3) and according to Table II the theoretical ranges that satisfy the demand response requirements in terms of number of GTS slots and probability of clear channel are bounded by (4,0.99), (5,0.7), (6,0.5), (7,0.3). In calculating these points the following parameters were used based on the ZigBee and SEP 2.0 specifications: b=508 bytes, C=250 kbps, BI=960 symbols.

f_6) Node Availability (NA): Represents whether or not health messages are received from the agents.

We choose these features for HANIDPS, since they well characterize the normal behavior of the system, at the same time considering that most of them (D, TR, SN, PER) are extracted from system specifications they do not result in a high FPR. Use of RSS feature enables the HANIDPS to detect and stop spoofing attack, which in wireless networks is an important attack type that can be used as a basis for several other attacks. The detection module evaluates each of the above features and if one of them is abnormal, an intrusion is detected and the prevention module is triggered. The results of the evaluation of these features are also used to define the state space for the prevention module. The components of the state space are defined as $\{f_1,...,f_6\}$ where f_i, i=1,...,6 are binary values, assigned by evaluating features 1-6. For each of D, TR, RSS, SN, PER and NA, C-IDPS checks whether or not the feature is normal, as described above, and accordingly assigns a binary value to f_i, 0 if the feature is normal and 1 if it is abnormal. The proposed intrusion detection method is robust against data encryption, since from the above features TR, SN, PER and NA are independent from the frame contents. Also D and TR are extracted from the header of MAC layer frames, while in IEEE 802.15.4 encryption is performed on data payload of MAC layer frames.

The decision epoch, i.e. the time interval between inferring the new state of the system to decide whether or not an attack is happening, defines the trade-off between the detection delay and the detection accuracy. The required time interval depends on the traffic rate, since for instance in evaluating the RSS feature the algorithm needs to receive and analyze n frames to decide if an attack is happening. The larger is the n the lower is the FPR and the higher is the DR. Yet increase of n means a longer delay in detecting the attack, which increases the chance of disturbance of the network by attackers. Therefore, this parameter must be adjusted based on the functional priorities and security requirements of the network.

C. Actions

a_1) Spoofing Prevention: In [7] we proposed an RSS based method for filtering illegitimate packets in static IEEE 802.15.4 networks. We use the dynamic threshold method introduced in [7] as a defense mechanism in HANIDPS. A brief explanation of the algorithm is as follows. RSS values of a node follow a Gaussian distribution. C-IDPS and agents calculate the mean and variance of RSS values of received frames for each communicating node under normal condition. When an alarm is received declaring the possibility of a spoofing attack, frames with RSS values that deviate from the mean value more than a threshold are dropped. To calculate the threshold, a queue containing the RSS values of n last frames is formed. Using 2-cluster K-means algorithm [7] the RSS values are divided into two clusters. Threshold value is assigned based on the distance between two cluster centers. For detail explanation of the algorithm we refer the readers to [7]. The AM is installed on C-IDPS and is only responsible for capturing the RSS values of network frames. C-IDPS then analyses the RSS values and decides whether a spoofing attack is happening. Once it detects a spoofing attack, it sends a message to agents which are installed on network nodes. The agents then filter malicious frames using the above mentioned algorithm.

a_2) Interference Avoidance: In [24] an algorithm for avoiding WiFi interference in ZigBee networks was proposed. The method is also effective in combating other sources of interference such as jamming. We adopt the interference avoidance scheme in [24] as one of HANIDPS preventive actions. Summary of the algorithm is as follows. C-IDPS checks its link quality indicator (LQI). LQI is a MAC layer parameter which indicates the current quality of received signals, and provides estimation on how easily received signals can be demodulated. LQI is inversely related to PER. When LQI is small, it can be inferred that a high PER is due to poor link quality rather than problems with end device. If the LQI is low the coordinator makes all the routers within the PAN to perform interference assessment through energy detection (ED) scans defined in ZigBee protocol. During an ED test, the transceiver scans all the IEEE 802.15.4 complaint channels in the frequency band supported by the transceiver. If ED is beyond the threshold

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2600585, IEEE Transactions on Smart Grid

of 35 (which corresponds to the noise level between -65 dBm to -51 dBm) interference is detected. Based on the results of ED scans the coordinator selects a channel with an acceptable quality and all PAN devices migrate to this new channel. In this work the network coordinator is the C-IDPS node which performs the interference avoidance operation.

a_3) Packet Drop: C-IDPS discards the packets which datagram or sequence numbers deviate from those predicted by the protocol without forwarding them to the intended destinations.

a_4) Packet Forward: C-IDPS forwards the received packets without further processing. This is helpful when an attacker targets the IDPS by sending high rate traffic to exhaust the IDPS and cause DoS. Another example is when none of the actions are effective in mitigating the attack and only impose overhead.

Using the actions introduced in this section enables HANIDPS to detect and stop a variety of attack types. It is possible to design mechanisms for stopping other attack types and add them as actions to HANIDPS. However, designing mechanisms to prevent all possible attacks against wireless networks is not in the scope of this work.

D. Learning Algorithm

After evaluating the network features, CIDPS infers the network state s and if an intrusion is detected by the detection module, it performs an action a which results in transition to a new state s'. The transition probability only depends on the current state and action, and is independent from all previous states and actions; therefore, satisfies the Markov property. Considering that attackers use different strategies to target the network, the interaction between HANIDPS and the attacker creates a dynamic environment, meaning that by taking an action in a given state, the next state is unpredictable. Therefore, among various existing reinforcement learning algorithms we use Q-learning which is suitable for dynamic environments. In Q-learning a utility function is defined as a map between the state-action pairs and their Q values. Q-values predict the cumulative reward that will be received following the state-action. When the state space is not too large a look up table (LUT) can effectively be used as the utility function. The LUT can be initialized by zero or based on previous knowledge of the environment. During the learning process the time is divided into decision epochs. In each epoch the agent chooses action a in state s which results in transition to state s' and receiving a reward or penalty based on how appropriate the transition is. After each epoch the LUT is updated using (5):

$$\begin{aligned} Q\left(s,a\right) = {} & Q\left(s,a\right) \\ & + \alpha\left(R\left(s,s',a\right) + max_{a'}\gamma Q\left(s',a'\right) - Q\left(s,a\right)\right) \end{aligned} \tag{5}$$

where α is the learning rate and γ is the discount factor. We use polynomial learning rate in which $\alpha = 1/(1+t)^{\omega}$ since it has a faster convergence rate compared to linear learning rate [25]. In our problem the state elements are binary values assigned based on whether or not the network features are normal. At state s, state elements are $\{f_1^s, ..., f_6^s\}$. At each state four actions described in Section IV-C are possible: spoofing prevention, interference avoidance, packet drop and packet forward. By performing action a in state s the process moves to state s' with state elements $\{f_1^{s'}, ..., f_6^{s'}\}$. To assess the new state, C-IDPS extracts and reevaluates the features of network traffic after performing the action. Following each action a reward is received based on the state transition as formulated in (6). We define the reward as a function of the changes in state elements and the cost of performing an action as follows:

$$R\left(s,s',a\right) = \sum_{i=1}^{6} \beta_i \left(f_i^s - f_i^{s"}\right) - cost\left(a\right) \tag{6}$$

where β_i is the weight of feature i which is assigned according to the importance of each feature. For instance, given that node availability might have more priority than having a normal traffic rate, by choosing $\beta_6 > \beta_2$, higher reward will be assigned to the action which keeps the node available. The cost function, $cost(.)$, reflects the costs associated with performing an action. It accounts the network overhead, imposed delay and resource usage such as battery consumption following performing an action. As a case in point, the cost of dropping packets is lower than changing the channel which results in some network overhead, delay and resource usage. While the LUT can be initialized randomly, there exist some relationship between the features and actions. For instance when the datagram does not comply with the specifications, dropping the packets might be a better choice compared to other actions. This knowledge can be employed to initialize the LUT to reduce the learning time. If actions a_2 or a_4 is selected, $\{f_1^{s"}, ..., f_6^{s"}\}$ are equal to the elements of the new state s'. Otherwise, if actions a_1 or a_3 is performed, C-IDPS reevaluates features f_1 to f_4 of the forwarded packets by the C-IDPS and accordingly defines $\{f_1^{s"}, ..., f_4^{s"}\}$. $f_5^{s"}$ and $f_6^{s"}$ are equal to $f_5^{s'}$and $f_6^{s'}$, respectively. We used this method because when actions a_1 or a_3 are performed C-IDPS drops some of the network packets and in order to decide how suitable these actions have been we need to evaluate some features of the forwarded packets rather than all of the network traffic.

V. Theoretical Analysis

A. Performance of the Detection Module

Among the 6 features used in HANIDPS to detect network abnormalities, 4 (D, TR, SN, PER) are directly extracted from system specifications and are not considered major sources of false positives. For instance, a healthy packet never has a D different from what the protocol defines. SN of legitimate packets also does not circumvent the specification. The probability of having a TR and PER beyond the threshold under normal condition is very low, since SEP 2.0 specified strict rules for traffic rates and network requirements. While ambient noise, temporary system faults or wireless communication faults can produce false positives in evaluating NA and some other features, the major cause of false positives in HANIDPS is the RSS evaluation results, since RSS is a statistical parameter and a trade off between FPR and DR is required. FPR of the

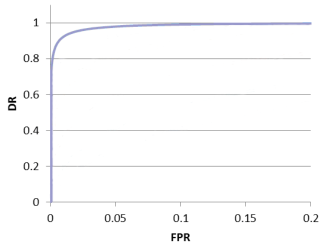

Fig. 2: ROC of the spoofing detection module for λ=40, σ=5 and 1 AM.

detection module is formulated as follows:

$$FPR = P\left(\bigcup_{i=1}^{6}(f_i = 1)|normal\right) \leq \sum_{i=1}^{6} P^i_{normal}\left(f_i = 1\right) \cong P^3_{normal}\left(f_3 = 1\right) \quad (7)$$

where P^i_{normal} is the probability distribution of i^{th} feature under normal condition. As we showed in [6]:

$$P^3_{normal}\left(f_3 = 1\right) = 1 - F_{\chi^2(m)}\left(\frac{\tau}{2\sigma^2}\right) \quad (8)$$

$\chi^2(m)$ is Chi-square distribution with m degrees of freedom which is equal to the number of AMs used in spoofing detection. HANIDPS uses one AM which is in the C-IDPS. $F_\chi(.)$ represents the CDF of χ , σ is the variance of RSS values and τ is a threshold. When τ is exceeded, a spoofing attack is detected. The detection rate (DR) of the spoofing detection module is:

$$DR = P^3_{attack}\left(f_3 = 1\right) = 1 - F_{\chi^2\left(m,\frac{\lambda}{2\sigma^2}\right)}\left(\frac{\tau}{2\sigma^2}\right) \quad (9)$$

where P^3_{attack} is the probability distribution of RSS feature under attack and λ is the distance between SDC distribution of the attacker and the genuine node. For further explanation on performance of the spoofing detection module we refer the readers to our previous work [6]. Fig. 2 shows the theoretical receiver operating characteristic (ROC) of the spoofing detection module. For other features attacks are only detectable if they create a network traffic that does not comply with the SEP 2.0 specifications. This, however, enables detection and prevention of a variety of attack types.

B. Performance of the Prevention Module

The intrusion prevention module performs two types of actions, training and operation.

1) Training actions: are taken for the purpose of training the Q-learning. They are selected before the algorithm is converged and are not effective in mitigating the attack. Hence, they mainly cause network and system overhead. Assuming a simple case when one action, a_i, is effective in mitigating the attack and T iteration is required before the algorithm converges, overhead of the learning algorithm is:

$$Overhead = \frac{1}{3}\sum_{t=1}^{T}\sum_{i=1,i\neq j}^{4} P_i(t)O(a_i) \quad (10)$$

where $P_i(t)$ is probability of choosing action i at iteration t and depends on the initial values, reward function and order of state/actions in LUT. $O(a_i)$ represents the overhead of performing action i. T is convergence time. In [25] convergence rate of Q-learning was studied. The authors showed that in asynchronous Q-learning with polynomial learning rate, aside from parameters of the Q-learning, convergence time is related to the covering time, L. Covering time indicates the number of state-action pairs starting from any pair, until all state-actions appear in the sequence with probability of at least 0.5. The order of this dependency is $\Omega(L^{2+\frac{1}{\omega}} + L^{\frac{1}{1-\omega}})$ which is optimized for $\omega = 0.77$. Having 6 binary features, the state space size of HANIDPS is 64; for each state there exist 4 possible actions. However, not all states are experienced during a specific attack. Number of states crossed during an attack, and therefore covering time depend on the attack complexity. The number of states can range from 2 when the attacker uses a specific attack type which follows a same routine over time, to a few when the attacker reacts and adjust his/her strategy according to the actions taken by HANIDPS. Our experiments in Section VI show that the algorithm converges with the required precision in few iterations which keeps the learning overhead in an acceptable range.

2) Operation actions: These actions are taken after the algorithm is trained and are chosen as the best defense mechanism against the attack.

2.1) Performance of Spoofing Prevention: In [7] we showed that the prevention rate (PR) and FPR of our proposed spoofing prevention method is:

$$PR = Q(\mu_g + \tau; \mu_a, \sigma_a) \quad (11)$$

where μ_g and μ_a are the mean RSS values of the genuine and the attacker nodes. τ is the threshold and Q is the Q-function (the complement of the CDF) of the Gaussian distribution.

$$FPR = 2\Phi(\mu_g - \tau; \mu_g, \sigma_g) \quad (12)$$

Φ is the CDF of the Gaussian distribution. The threshold defines the trade-off between PR and FPR. The larger the threshold the smaller is the FPR, yet it also provides a smaller PR. False positives introduce network overhead, since when a genuine frame is dropped due to exceeding the RSS threshold, several retransmissions might be required until the RSS lies within the legitimate range. The expected number of retries until a successful transmission is formulated as:

$$E = \frac{1}{1 - 2\Phi\left(\mu_g - \tau; \mu_g, \sigma_g\right)} \quad (13)$$

Fig. 3 shows the relation between E and FPR, which also represents the effect of FPR on network overhead. Fig. 4 shows the ROC curve for different distances between RSS mean values of the attacker and genuine nodes. When threshold is assigned dynamically based on the difference between RSS mean values, not only attacks with close distance to the genuine node are preventable, but also unnecessary network overhead is avoided. Detailed performance analysis of the spoofing prevention algorithm was provided in our previous work [7]. Delay of the spoofing prevention module depends

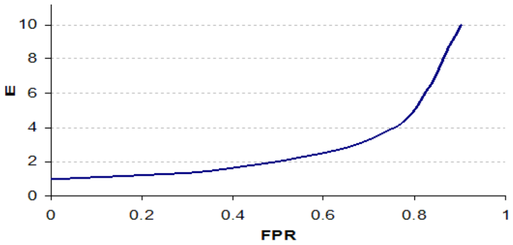

Fig. 3: Expected number of retries for a successful transmission vs. FPR.

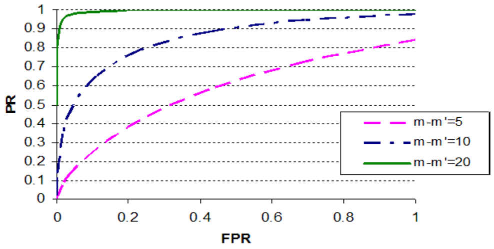

Fig. 4: Theoretical ROC of spoofing prevention (m and m' are the mean RSS values of the genuine and attacker nodes).

on the queue size for calculating the threshold and traffic rate.

2.2) Performance of Interference Avoidance: Experiment results in [24] showed that with the ED scan duration of 135 ms, the proposed algorithm provides the best balance between scan duration and accuracy. During this time network nodes cannot transmit normal traffic. In return, the authors showed that by choosing a less interfered channel, the sensors battery life can be prolonged by up to 2-3 years; while if the network operates under high interference, a high PER will result in a large retransmission rate which wastes the energy of sensors. The other two actions including packet forward and packet drop does not impose significant delay or overhead.

VI. Evaluations

To evaluate the performance of HANIDPS, we study existing attacks against IEEE 802.15.4 networks and analyze the detection and prevention capability of HANIDPS against them. Further, we conduct two experiments to show how HANIDPS dynamically learns the most efficient strategy against an attack.

A. HANIDPS against IEEE 802.15.4 attacks:

1) Radio Jamming: Radio jamming is intentional or unintentional emission of radio signals which by decreasing the signal to noise ratio disturb data flow of a wireless network. When the network is under jamming, PER and NA are not in the expected range. High interference increases the PER, and since nodes are not able to communicate properly, health messages will not be received by the C-IDPS. When these two features of the feature space are abnormal, HANIDPS detects an attack and triggers the prevention module. From the actions defined for the HANIDPS, interference avoidance is effective in stopping unintentional jamming. C-IDPS changes the network channel to a new high quality one. Coexistence of WiFi networks is one of the significant concerns in ZigBee HANs [24], since high rate WiFi traffic can cause unintentional jamming. When jamming is unintentional the interfering device will not change its channel and therefore by migrating to a new channel the problem is resolved. This is also true for simple cases of intentional jamming. But in more complicated attacks, for instance when the attacker also changes its channel or conduct a wide band jamming which covers the whole ZigBee frequency range, interference avoidance scheme will not be effective. Yet these attacks are more expensive and energy consuming.

2) Replay-protection: IEEE 802.15.4 uses a replay-protection mechanism in which sequence number of a received frame is compared with sequence number of the previous frame. If the former is equal or smaller than the latter the frame will be dropped. An attacker can send frames with large sequence numbers to a receiver, causing it to drop legitimate frames. The detection module checks the sequence numbers. If they do not comply with the standard, SN feature will be abnormal and the attack will be detected. By dropping illegitimate packets, which is one of the HANIDPS actions, this attack can effectively be stopped. The prevention module learns the proper action after a few iterations.

3) Steganography: An attacker uses the reserved fields of packets to create a hidden channel and transfer hidden data. A detailed investigation of steganography attacks in IEEE 802.15.4 was reported in [26]. HANIDPS checks datagram of packets and if it is abnormal (for instance when reserved bits are not 0 as it happens in steganography) detects an attack. The effective action against this attack is dropping malicious packets which is learned through reinforcement learning and performed by the prevention module in HANIDPS.

4) Back-off manipulation: A malicious node steals channel access of legitimate nodes by using an instantly short back-off period. The malicious node is either one of the network nodes that has been penetrated, or an outside node which forges ID of legitimate nodes and conducts spoofing to access the network. In both cases the attacker has a very high traffic rate and TR for that node will be 1. Also since nodes are not able to transmit their packets properly, health massages might not be received by C-IDPS and NA will be 1. Beside, not being able to access the channel increases the PER. In the case of spoofing, RSS values are not normal either. By causing abnormal TR, NA, PER and RSS the attack is easily detectable. The prevention module can mitigate the attack by filtering high rate traffic from the attacker and not allowing the coordinator to assign the channel to that node. Another action that can be helpful, in case of abnormal RSS values, is spoofing prevention. Through interaction with environment and receiving rewards and penalties HANIDPS converges to the best action.

5) DoS against data transmission during contention free period (CFP): A malicious node extracts ID and GTS number of legitimate nodes through eavesdropping; then forges their IDs and by sending GTS deallocation requests terminates their traffic [27]. Since the malicious and genuine nodes are not located at the same place, their RSS values will not be similar

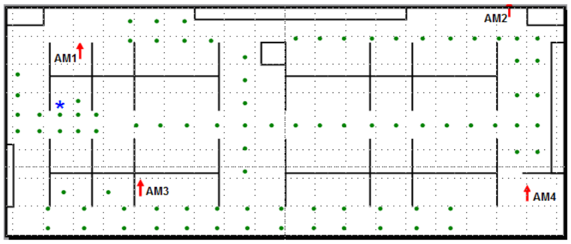

Fig. 5: Testbed setting (the distance between consecutive grid dots is 50 cm).

and the attack is detectable by evaluating RSS feature. Also through spoofing prevention action, packets with abnormal RSS values are filtered. Therefore, once the prevention module learns what the appropriate action is, the attack is stopped.

6) DoS against GTS requests: An adversary keeps track of the GTS list and fills up all available GTSs by sending several GTS allocation requests. As a result, legitimate nodes will not have the chance to transmit their data during CFP [27]. Since RSS of the attacker does not match that of the genuine node, the attack is detectable and through spoofing prevention malicious packets can be dropped.

B. Experiment 1

We study the performance of HANIDPS under a simple spoofing attack where other than RSS values traffic features of malicious node is consistent with the protocol. DoS against GTS requests is an example of this attack.

1) Test bed: We established an IEEE 802.15.4 network in an office building in the Electrical and Computer Engineering Department of the University of British Columbia. The network contained six nodes, including 4 AMs, an attacker and a genuine node. TelosB motes were used as network nodes. The AMs were programmed to monitor and save RSS of received frames. The attacker and the genuine nodes were programmed to send constant bit rate (CBR) traffic with 5 frames per second rate. Fig. 5 shows the network map in which AMs are depicted by arrows and the genuine node by a star. During the experiment the attacker node was placed in different locations shown by bold dots (five minutes in each position). RSS logs were collected and analyzed at the end.

2) Performance of the detection module

By applying the spoofing detection mechanism on RSS logs, in average we observed 92.5% DR for 0% FPR. The average ROC curve based on RSS logs of 4 AMs is depicted in Fig. 6. When the attack is detected the state of the victim node is {0,0,1,0,0,0} which triggers the prevention module.

3) Performance of the prevention module

Training Phase: We implemented Q-Learning in MATLAB. The LUT was initialized by 0.5. We considered the same weight for all features, and assigned the cost values of 0.25, 0.5, 0.1, 0 to actions 1-4, respectively. The highest cost was defined for interference avoidance since it is an energy consuming process. The first four actions were exploratory [25]. Then we reduced the exploration rate by a factor of $\frac{1}{4}^{\left[\frac{i}{4}\right]}$ as the algorithm proceeded (i is the number of iteration).

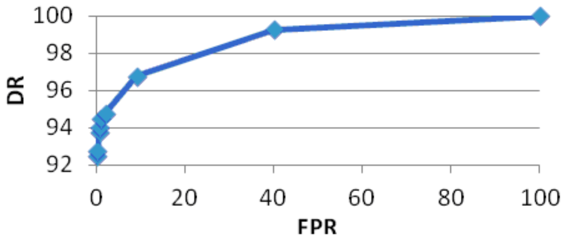

Fig. 6: ROC of the detection module.

TABLE III: Performance of dynamic threshold spoofing prevention.

Threshold coefficient	1/2	1/3	1/4	1/5
PR(%)	93.46	96.07	97.14	97.62
FPR(%)	6.16	11.17	16.21	21.68

Use of exploratory actions allows the algorithm to explore all actions and converge to the most effective ones. The learning rate was polynomial with $\omega = 0.77$ and the discount factor was $\gamma = 0.1$. Following the spoofing prevention action the state of the node was changed to {0,0,0,0,0,0} while for other actions the state remained unchanged. We observed that for this simple case where only two states are experienced, the algorithm learns the best action after 4 iterations.

Operation phase: We evaluated the performance of the spoofing prevention mechanism as the effective action against the attack. We applied the spoofing prevention algorithm to RSS logs. This time the AM nodes played the role of a victim. Performance was measured when the threshold was 1/2, 1/3, 1/4 and 1/5 of the distance between the mean values. The window size, i.e. the number of frames which are clustered each time was 64. Results are shown in Table III.

C. Experiment 2

In this experiment our goal is to evaluate the ability of HANIDPS in choosing the most efficient action to mitigate the attacks. Therefore, in this experiment we consider a scenario in which two of the actions defined for HANIDPS can help to stop the attack. During the attack an adversary forges the ID of a legitimate node to send traffic on its behalf, but this time packets that are sent by the attacker do not comply with the protocol standard. For instance, they have a larger packet size or use some of the reserved fields to send data. Steganography is an example of the latter. When the system is under the attack RSS and D features are abnormal and the state of the victim node is {1,0,1,0,0,0}. Both Spoofing Prevention and Packet Drop actions (a_1 and a_3) can stop the attack and change the state to {0,0,0,0,0,0}. However, a_3 imposes less overhead since it requires less computations and processing time.

To simulate the prevention module of HANIDPS, we implemented the Q-learning in MATLAB. We initialized the LUT and chose the parameters of Q-learning the same as Experiment 1. We observed that the algorithm converged to chosing a_3 after four iterations. The reason why between a_1 and a_3 the algorithm converged to a_3 is that the costs of these actions in the formula for calculating the rewards were

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2600585, IEEE Transactions on Smart Grid

defined 0.5 and 0.1, respectively. Therefore, the algorithm receives a higher reward for performing a_3 and after some iterations converges to this action. This shows that through careful calculation of the cost of performing each action, we can bias the algorithm toward choosing the most efficient one.

VII. Discussion

It is possible that attackers use some techniques such as imitation attacks to evade the IDS. In the following we analyze the performance of HANIDPS against existing evasion techniques for network IDSs.

- *Obfuscation:* By obfuscating or encoding the payload in a way that it is reversible by the end system but not the IDS, an attacker can evade the IDS. HANIDPS is designed for PHY and MAC layers, and it does not check the payload of messages. therefore, obfuscation does not affect its performance.
- *Fragmentation:* In this method the payload is split into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. One of the features that HANIDPS checks is datagram of packets including packet length. Considering that HANIDPS works based on the features of layers 1 and 2 of the network, it does not check the content of the payload and it does not reassemble the packets. Therefore, if an attack does not affect any other features of the network it will not be detected by HANIDPS.
- *Protocol Violation:* In this method, the protocol is deliberately violated in a way that the target system will handle it differently from the IDS. For instance, on different operating systems the TCP Urgent Pointer is handled differently and may not be handled correctly by IDS. Considering that the number of protocols and applications in HAN is limited, through careful development of software codes these attacks can easily be avoided.
- *Inserting traffic at the IDS:* An attacker sends packets to the IDS but not other nodes. Thus, the state of the IDS will be different from the state of the target system. For example, the Time to Live field of the message can be modified so that the message reaches the IDS but not the target node. This attack is suitable for stateful IDSs which are designed for upper layers of the network protocol stack and monitor the flow and order of transferred messages. HANIDPS is designed for the lower layers of network and its performance is independent from the order of the network messages. Therefore, this attack does not affect its performance.
- *DoS:* The attacker exhausts the IDS through using up computational resources or exploiting a bug in the IDS. The bugs in the IDS can be avoided through careful development and test of the software codes. Moreover, since HANIDPS works in lower layer of network it has short delay and requires low computation for attack detection. Therefore, exhausting its resources is not easy for attackers.

VIII. Conclusion

In this work we have introduced HANIDPS, a novel IDPS for ZigBee-based HANs. Considering the insecure environment, use of wireless technology and limited resources of HAN devices, HAN is vulnerable to cyber attacks which necessitates application of appropriate IDSs. Also due to the large scale and high cost of false positives, IDPSs which not only detect but also automatically stop the attacks are highly required. HANIDPS combines a model-based intrusion detection method tailored for HAN specifications and a machine learning-based prevention technique which enables dynamic defense against adversaries without prior knowledge of the attacks. Using novel techniques for spoofing prevention, and through utilization of effective mechanism against intentional and unintentional interference, HANIDPS secures the network against a variety of attack types. Extensive analysis and simulations have proved the effectiveness of our approach.

IX. Acknowledgment

This work was supported in part by UBC Graduate Support Initiative award, the Canadian Natural Sciences and Engineering Research (grants RGPIN-2014-06119 and RGPAS-462031-2014), and by the National Natural Science Foundation of China (Grant 61271182).

References

[1] NISTIR 7628 Rev. 1, Guidelines for smart grid cyber security, 2014.

[2] J. Wright, Smart meters have security holes, http://www.msnbc.com/id/36055667, 2010.

[3] FBI: Smart meter hacks likely to spread, http:// krebsonsecurity.com /2012/04/fbi-smart-meter-hacks-likely-to-spread

[4] Smart energy profile 2.0 application specification document, 2012.

[5] P. Jokar, H. Nicanfar and V. C. M. Leung, Intrusion detection system for home area networks in smart grids, *Second IEEE International Conference on Smart Grid Communications*, 2011.

[6] P. Jokar, N. Arianpoo and V. C. M. Leung, Spoofing detection in IEEE 802.15.4 networks based on received signal strength, *Elsevier Ad Hoc Networks*, vol. 11, no. 8, pp. 2648-2660, 2013.

[7] P. Jokar, N. Arianpoo and V. C. M. Leung, Spoofing prevention using received signal strength for ZigBee-based home area networks, *IEEE SmartGridComm*, 2013.

[8] R. Mitchell and R. Chen, Behavior-rule based intrusion detection systems for safety critical smart grid applications, *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp.1254-1263, 2013.

[9] L. Wang, W. Sun, R. C. Green and M. Alam, Distributed intrusion detection system in a multi-layer network architecture of smart grids, *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796-808 , 2011.

[10] C. H. Lo and N. Ansari, CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid, *IEEE Trans. on Emerging Topics in Computing*, vol. 1, no. 1, pp. 33-44, 2013.

[11] P. Y. Chen, S. Yang, J. A. McCann, J. Lin and X. Yang, Detection of false data injection attacks in smart-grid systems, *IEEE Communications Magazine*, vol. 53, no. 2, pp. 206-213, 2015.

[12] N. B. Mohammadi, J. Misic, H. Khazaei and V.Misic, An intrusion detection system for smart grid neighborhood area network, *ICC*, 2014.

[13] R. Berthier and W. H. Sanders, Specification-based intrusion detection for advanced metering infrastructures, *IEEE Pacific Rim International Symposium on Dependable Computing*, 2011.

[14] M. Q. Ali, R. Yousefian, E. Al-Shaer, S. Kamalasadan and Q. Zhu, Two-tier data-driven intrusion detection for automatic generation control in smart grid, *IEEE CNS*, 2014.

[15] S. Parthasarathy and K. Deepa, Bloom filter based intrusion detection for smart grid SCADA, *IEEE Canadian Conference on Electrical and Computer Engineering*, 2012.

[16] N. Goldenberg and A. Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 63-75, 2013.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2600585, IEEE Transactions on Smart Grid

[17] K. Ioannis, T. Dimitriou and F. C. Freiling, Towards intrusion detection in wireless sensor networks, *European Wireless Conference*, 2007.

[18] R. Berthier, W. H. Sanders and H. Khurana, Intrusion detection for advanced metering infrastructures: requirements and architectural directions, *IEEE SmartGridComm*, 2010.

[19] F. Tabrizi and K. Pattabiraman, A model for security analysis of smart meters, *IEEE/IFIP Conference on Dependable Systems and Network Workshops*, 2012.

[20] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier and P. McDaniel, Multi-vendor penetration testing in the advanced metering infrastructure, *ACM Computer Security Applications Conference*, 2010.

[21] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. Cardenas and J. G. Jetcheva, intrusion detection requirements and deployment recommendations, *IEEE Conference on Smart Grid Communications*, 2012.

[22] U.S. Department of Energy, Communications requirements of smart grid technologies, pp .169, 2010.

[23] V. Kounev and D. Tipper, Advanced metering and demand response communication performance in ZigBee based HANs, *INFOCOM*, 2013.

[24] P. Yi, A. Iwayemi and C. Zhou, Developing ZigBee deployment guideline under WiFi interference for smart grid applications, *IEEE Trans. on Smart Grid*, vol. 2, no. 1, pp. 110-120, 2011.

[25] E. Even-Dar and Y. Mansour, Learning rates for Q-learning, *Journal of Machine Learning Research*, vol. 5, pp 1-25, 2004.

[26] D. Martins and H. Guyennet, Attacks with steganography in PHY and MAC layers of 802.15.4 protocol, *International Conference on Systems and Networks Communications*, 2010.

[27] R. Sokullu, O. Dagdeviren and I. Korkma, On the IEEE 802.15.4 MAC layer attacks: GTS attack, *Sensor Technologies and Applications*, 2008.

Paria Jokar (M'2010) received her B.Sc and M.Sc. degree with distinction in electrical engineering from the Iran University of Science and Technology. She is currently working toward Ph.D. in the Department of Electrical and Computer Engineering, University of British Columbia, Canada. Her Research interests include networks and network security.

Victor C. M. Leung (S'75-M'89-SM'97-F'03) received the B.A.Sc. (Hons.) degree in electrical engineering from the University of British Columbia (UBC) in 1977, and was awarded the APEBC Gold Medal as the head of the graduating class in the Faculty of Applied Science. He attended graduate school at UBC on a Natural Sciences and Engineering Research Council Postgraduate Scholarship and completed the Ph.D. degree in electrical engineering in 1981.

From 1981 to 1987, Dr. Leung was a Senior Member of Technical Staff and satellite system specialist at MPR Teltech Ltd., Canada. In 1988, he was a Lecturer in the Department of Electronics at the Chinese University of Hong Kong. He returned to UBC as a faculty member in 1989, and currently holds the positions of Professor and TELUS Mobility Research Chair in Advanced Telecommunications Engineering in the Department of Electrical and Computer Engineering. Dr. Leung has co-authored more than 900 technical papers in international journals and conference proceedings, 31 book chapters, and co-edited 11 book titles. Several of his papers had been selected for best paper awards. His research interests are in the areas wireless networks and mobile systems.

Dr. Leung is a registered Professional Engineer in the Province of British Columbia, Canada. He is a Fellow of IEEE, the Royal Society of Canada, the Engineering Institute of Canada, and the Canadian Academy of Engineering. He was a Distinguished Lecturer of the IEEE Communications Society. He is a member of the editorial boards of the IEEE Wireless Communications Letters, IEEE Journal on Selected Areas in Communications Series on Green Communications and Networking, IEEE Access, Computer Communications, and several other journals, and has previously served on the editorial boards of the IEEE Journal on Selected Areas in Communications - Wireless Communications Series, IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology, IEEE Transactions on Computers, and Journal of Communications and Networks. He has guest-edited many journal special issues, and provided leadership to the organizing committees and technical program committees of numerous conferences and workshops. He was a recipient of the IEEE Vancouver Section Centennial Award and 2012 UBC Killam Research Prize.