Model-based Intrusion Detection for Home Area Networks in Smart Grids

Paria Jokar

Department of Electrical and Computer Engineering

University of British Columbia

Vancouver, Canada
pariaj@ece.ubc.ca

ABSTRACT

In this paper we present a model-based intrusion detection system (IDS) for home area networks (HANs) within the smart grid. Considering that ZigBee is the dominant technology in future HAN, the proposed IDS is designed to target ZigBee standard. Our focus is on the physical and medium access control (MAC) layers of ZigBee technology, which are defined in IEEE 802.15.4 standard. In the proposed IDS, normal behavior of the network is modeled through specifications extracted from the IEEE 802.15.4 standard as well as features of wireless network traffic. Deviations from normal behavior can be a sign of malicious activities. We use Bayesian network as a classifier to distinguish the normal and malicious behavior of the network according to extracted features. We further investigate the physical and MAC layer attacks in IEEE 802.15.4 networks that have been introduced in literature. In order to evaluate the performance of the proposed method we simulate a HAN network as well as some attack scenarios, in NS-2 simulation environment. We evaluate the performance of the proposed IDS against these attacks. Analysis and simulation results demonstrate that the proposed IDS provides good detection performance against known attacks, and since this is an IDS based on anomalous event detection, we expect the same for unknown attacks.

Keywords

HAN, IDS, smart grid

1. INTRODUCTION

Smart grid is a vision to modernize the electricity transmission and distribution systems. Smart grid incorporates computer intelligence into the power system, and provides two way energy flow and data communication. Unlocking the tremendous potential of the smart grid such as resilience, high power quality, and consumer participation, strongly depends on the security of this system. Integration of a data layer to the power grid can expose the system to many cyber security threats. Smart grid is an infrastructure that many other utilities rely on; without strong security measures, not only the smart grid will inherit the vulnerabilities of the legacy power system, but also new vulnerabilities will be added due to the proliferation of new technologies.

In the 2009 White House Cyberspace Policy Review, federal government was asked to "ensure that security standards are developed and adopted to avoid creating unexpected opportunists to penetrate these systems or conduct large-scale attacks" [1]. The US National Institute of Standards and Technology (NIST) has provided guidelines for developers and policy makers, covering cyber security requirements of the smart grid that should be included from the beginning of the development process [2]. Along with the security mechanisms that should be designed into the smart grid with the goal of reducing the vulnerabilities and mitigating their consequences, such as cryptographic algorithms and secure protocols, appropriate intrusion detection systems (IDSs) are also required. The need for research on intrusion detection for embedded processors has been emphasized in "NIST guidelines for smart grid cyber security", in that smart grid contains a large number of processors with limited resources and strict timeliness requirements.

Smart grid deployments are divided into three domains: Advanced metering infrastructure (AMI), distributed generation, wide area measurement and control. AMI provides two-way communication between smart meter and utility company which enables real-time transmission of power consumption and pricing data, as well as control commands. Home area networks (HANs) are subsystems within AMI which are responsible for data transfer among the smart meters and household electric devices and appliances. In many countries wireless is the dominant technology for HAN. The shared media used by wireless networks make them inherently more vulnerable to security threats compare to wired networks. In addition, HAN is located in the public domain, which makes it an easily accessible target for malicious attackers. At the same time, due to the resource and computational limitations of HAN devices implementation of strong security mechanisms is a challenging issue. Therefore, employment of appropriate IDS tailored for HAN based on its requirements, limitations and characteristics is necessary.

In this paper we introduce a model-based IDS for HAN. The remainder of the paper is organized as follows: Section 2 provides literature survey on related research area. Section 3 addressed HAN security challenges and requirements. Section 4 describes the design of our proposed IDS. A survey on existing attacks against IEEE 802.15.4 is provided in Section 5. In section 6 the performance of the proposed IDS is evaluated. We discuss some challenges and limitations of our work in Section 7 and Section 8 concludes the paper.

2. RELATED WORK

Conventional IDSs are unable to adequately address the unique requirements of the smart grid. Kush et al. [3] analyzed the gap between contemporary IDSs and the appropriate IDSs for smart grid. Authors of [3] explained the objectives of the smart grid and accordingly defined the IDS requirements in the context of smart grid, such as scalability, support of legacy protocol, adaptability, etc. They have further explained how the existing IDSs lack these requirements.

A hierarchical and distributed architecture for intrusion detection in smart grid has been proposed in [4]. In this architecture, the distributed IDS components are connected through a wireless mesh network. All IDS components in different hierarchies apply support vector machine (SVM) and immune system for detecting intrusions. The authors evaluated the performance of their IDS using KDD99 dataset.

In [5] Berthier et al. have investigated the requirements and challenges of monitoring and intrusion detection for AMI communication networks. They reviewed existing monitoring and IDS solutions and concluded that considering the scale, precision requirements and limited number of protocols, distributed monitoring and specification-based intrusion detection is an appropriate approach. The work in [5] looks at the whole infrastructure in general without focusing on AMI subsystems.

An IDS for SCADA system in the oil and gas industry, which is also extendable to the electricity industry, has been introduced by Roosta et al. in [6]. Since these systems have well-defined communication and regular traffic pattern, the authors have suggested a distributed, multi-layer and model-based approach. In their proposed method eight policy rules have been established to define normal behavior of physical, data-link and network layers. Theoretically, these policy rules can detect a wide range of cyber-attacks. The authors did not provide experimental evaluation to support the efficiency of their proposed method.

In [7], the feasibility of traffic-based intrusion detection in an IEEE 802.15.4 compliant sensor cluster has been evaluated. The authors used exponential traffic averaging to detect anomalous behavior of the network. They introduced a small hysteresis in the decision process to decrease false negative rate. This IDS is capable to detect attacks which affect the network traffic load.

In [25], we studied the architecture of HAN and proposed a specification based intrusion detection approach for HAN. This work is an extension of our previous work. Some changes in current work compare to [25] are: we take a more accurate look at HAN architecture and requirement of IDS for HAN, we optimize the feature space and include some statistical features, we apply a more effective classification scheme and we evaluate the performance of our IDS against some existing attacks.

Since 1995 several classification techniques have been adopted for intrusion detection, including neural networks [8], genetic algorithms [9], state transition [10], immune system [11], Bayesian network [12], fuzzy logic [13], hidden Markov models [8], decision tree [14]. A comprehensive study on anomaly-based IDS has been provided in [26]. Among available approaches, in the area of our work we are particularly interest in Bayesian network classifier which was first introduced in [12]. Bayesian network classifier consists of a number of models with interdependencies. According to the system features, and by use of conditional probabilities, models collaborate to make decision about the system status. The major advantage of Bayesian network IDS is that is does not require prior knowledge of malicious attacks, yet by accurate design it can maintain a low false positive rate. We have employed Bayesian network classifier in our IDS.

3. HAN

3.1 HAN Architecture

HANs are subsystems within AMI which are responsible for transferring usage data and control commands among smart meters and household electric devices. When customers know how much energy they are consuming per device and how much this energy will cost them in a given time, they might change their usage pattern willingly. Utilities also might have the right to turn off or reduce energy consumption of a specific device in HAN automatically for a short period of time by transmitting control signals to HAN devices through smart meters. This can be a great help for electric utilities to deal with overload caused by peak electricity demands. However, this level of automation which relies on the underlying data communication network exposes the system to cyber security threats.

Power efficiency is one of the major goals of smart grid; therefore, the communication technology behind the smart grid should use as low power as possible. In North America, Australia, Germany, and UK, wireless is the dominant technology for HAN, while in many other countries, especially in Europe, power line carrier (PLC) is the leading HAN technology. According to a study by General Electrics, between WiFi (802.11n) and ZigBee (802.15.4), which are the two technologies that best meet the HAN requirements, ZigBee is at least two times more cost-effective and efficient [15]. In fact, in North America ZigBee has become the leading standard for wireless HAN interface, which is why in this paper we develop our IDS based on IEEE 802.15.4 standard. IEEE 802.15.4 defines PHY and MAC specifications of ZigBee.

3.2 HAN Security

AMI infrastructure assets are divided into the private and public domains. The private domain includes systems that are similar to standard information technology (IT) assets. These systems contain a large amount of critical data; yet they are located in data centers which are secure environments. HAN on the other hand is located in the public domain, which is physically an insecure environment. Ease of accessibility of HAN devices makes them easier targets for attackers. At the same time, due to the resource and computational limitations of HAN devices implementation of strong security mechanisms is a challenging issue. For example, the sensor nodes in appliances might not be able to support computationally heavy cryptographic algorithms. Employing the wireless technology for HAN raises another security concern. The shared media used by wireless networks makes them inherently more vulnerable to malicious activities, such as eavesdropping and interference, compared to wired networks.

Many people with different motivations might aim to compromise the integrity, confidentiality and availability aspects of HAN security. An unethical customer, who wants to reduce his electricity charge, or to gain control of a special appliance, which according to the customer-utility agreement is under the control of the utility, might manipulate the usage reports or control signals. An adversary might send fake control signals to the HAN appliances to simply disrupt the service availability of his neighbor or to perpetrate more malicious intentions. An eavesdropper might listen to the network traffic to gain valuable information about the energy usage of a household.

Some consequences of penetrating to the HAN include:

Disturbing Service Availability: An attacker can disturb the service availability of a customer by sending false control signals to the sensor nodes or false usage data to the smart meters.

Although in most computer systems among confidentiality, integrity and availability, availability usually gets the lowest priority, in the context of power system the opposite is true. In fact one of the major goals of migrating to smart grid is to enhance the service availability.

Economic Loss: Penetrating to the HAN can cause economic loss to the utilities. By manipulating the usage data, customers can falsify the report of their energy consumption. Hence they will get lower electric charges compare to their real consumption charges.

Privacy Invasion: Customers' concern about their privacy is one of the major obstacles to the smart grid public adoption. In the smart grid more detailed energy usage data is collected through smart meters at much shorter time intervals. By penetrating to the HAN and reading the usage data one can deduce important information about the consumers, ranging from the type of household devices and appliances to information about the number of individuals in a house and their specific activities.

Penetrating to More Critical Assets: The traditional electric power grid is divided into three primary networks: generation, transmission and distribution networks. Smart grid intends to extend the distribution network to include HAN. Thus one can look at HAN as an entry point to the power system. According to [3] HAN is the easiest entry point to AMI for cyber attackers.

In summary HAN can inherently be an insecure system. At the same time it is the target of several attackers with a variety of motivation. Penetrating to the HAN can cause sever consequences. Therefore, presence of an IDS as the second line of defense against cyber threats seems necessary.

3.3 IDS requirements for HAN

As it is defined in [16], "intrusion detection is the process of monitoring the events that occur in a computer system or network and analyzing them for signs of possible incidents." In general, there are three types of IDSs based on the method they use for recognizing intrusions:

1) Signature-based IDS usually has a database of predetermined attack patterns, known as signatures, and detects the intrusions by comparing the system behavior with these signatures.
2) Anomaly-based IDS detects malicious activities as deviation from statistically normal behavior of the system.
3) Specification-based IDS also recognizes intrusions as deviation from normal behaviors of the system. However, instead of statistical measurements, normal behaviors are defined based on manually extracted specifications of the system.

Signature-based IDS has low false positive rates, yet it is incapable of detecting unknown attacks and its database should be updated frequently. Anomaly-based IDS on the other hand, suffers from high rate of false positives and long training and tuning time, yet it is able to detect unknown attacks. Specification-based IDS potentially has low false positive rates, and the ability to detect new attacks. However, the strength of this type of IDS depends on the accuracy and efficiency of the selected specifications. This type of IDS is more applicable to specific problems like mobile ad hoc networks compare to large systems with different protocols and applications such as the Internet.

Considering that many of the smart grid deployments including HAN devices are new technologies, an exhaustive database of attacks is not available. High update rate of signatures is another problematic issue. Thus, signature-based IDS will not be effective. Since a HAN supports only a few applications employing a limited number of protocols, it might be possible to establish a comprehensive set of specifications for it. Whenever possible, specification-based approach has higher priority than anomaly-based approach, since it potentially has a lower false positive rate.

While existing intrusion detection mechanisms can be used as a basis of developing IDS for HAN, the difference between HAN and the networks the IDSs are designed to address should be considered. HAN is different from computer networks in that HAN devices are sensor nodes with limited computational and processing resources. Moreover, unlike computer systems HAN devices support few numbers of protocols and applications. HAN is also different from many existing sensor networks where a large number of sensor nodes are spread over a vast hostile area. Typically HAN has relatively fewer numbers of nodes and a smaller coverage area. In designing IDS for HAN such differences should be considered.

Also in developing IDS for HAN one should consider the following question: who is responsible to receive the IDS reports and take action in response to intrusion detection alarms? Since customer can benefit from compromising the HAN, we assume that customer can be the adversary. Therefore, customers can not be trusted and utility should take the responsibility of managing the IDS reports. Although each HAN is relatively a small network, a smart grid contains a very large number of HANs. Even few false alarms per HAN will impose a huge operational cost on the utility. One can argue that in trade-off between false alarm and accuracy, a higher weight should be assigned to false alarm when it comes to intrusion detection for HAN. Beside the operational costs, when false alarm rate is high, true might be neglected by administrators. In [16], false alarm is introduced as the limiting factor for performance of an IDS. [16] emphasizes that although in many literature false positive rate, *P(Alarm | -Intrusion),* and accuracy, *P(Alarm | Intrusion),* are applied to evaluate the performance of an IDS, Bayesian detection rate, *P(Intrusion | Alarm)*, is a more concerning factor. The authors showed that in a typical computer network, for an IDS with 100% accuracy and 0.1% false negative rate, when IDS triggers a detection alarm the probability of occurrence of an intrusion is not more than 2%. To increase the ratio of correct alarms to 50%, the false negative rate should be less than 0.0001%. Considering the scale of the smart grid this effect should be addressed in designing IDS. For example in the distributed AMI IDS in [4], the best false positive rate is reported to be 0.67%. Adding the fact that the authors used KDD99 to evaluate the performance of their IDS, which repeatedly is reported to provide optimistic results [17], such performance might not be satisfactory for HAN.

Despite the popularity of machine-learning based intrusion detection in academic research, such approaches have not been adopted in practical and commercial applications. While in other domains, such as recommender systems, machine learning solutions have been successfully deployed in large scale. The gap between academic research and actual deployment is comprehensively addressed in [17]. Authors find the following factors responsible for this phenomenon: high cost of errors, lack of adequate training data, semantic gap between result and their operational interpretation, enormous variability in input data, and fundamental difficulties for sound evaluation. Unless these parameters be addressed, IDS solutions based on machine learning will not be effective.

4. HAN IDS

The proposed IDS contains two components: Monitoring agent and central IDS. Monitoring agents are installed on sensor nodes, and are responsible for monitoring the behavior of the corresponding node. Each agent collects information about the behavior of its sensor and sends reports to the central IDS in predetermined time intervals. In the proposed IDS the agents calculate the ratio of power consumption and the number of dropped packets by the corresponding node. The central IDS is implemented in a tamper resistant super node, with higher capacity and computational power compare to normal nodes. The central IDS listens to the packet stream to and from the PAN coordinator and extracts the features of network traffic. The combination of these features and the content of agent reports constitute the complete feature vector. Feature vector is then passed to the IDS classifier, where based on the predefined normal behavior of the network, the feature vector is classified to either normal or anomalous.

Based on the requirements of intrusion detection for HAN, explained in Section 3.3, we use a combination of anomaly and specification-based approaches. We choose eleven features to monitor the behavior of the system. Our IDS employs Bayesian-network classifier where a model is assign to each feature. The normal properties of features are defined for models in term of conditional probability tables. We use specification-based model as long as possible, however, justifying some features as specifications requires strong assumptions that might be limiting. In that case we use anomaly approach. Each model acts as an anomalous detector for its corresponding feature. The final decision is made based on the output of all the features. Following the discussion in Section 3.3, we avoid using machine learning approaches such as SVM. However, instead of simple threshold, or Naïve Bayesian classifier, we use Bayesian network which by accurate design has the potential to reduce the false negative rate significantly.

In the following subsections we describe the feature space, as well as the classification algorithm in our IDS.

4.1 Feature Space

Defining an appropriate feature space is the most important task in designing a model-based IDS. Feature space should accurately represent the normal behavior of the system; therefore, an exhaustive set of system specifications should be employed. At the same time resource and time limitations should be considered. Hence redundant features must be avoided. We choose eleven features that we believe are required to model the normal behavior of the system. In defining the feature space we use a layered approach, in this work we cover physical and MAC layers (Layer 1 and 2 orderly). Extracting some of the features only rely on monitoring the network traffic. Other features require monitoring of the sensor nodes. While relying only on network features has several advantages, agent characteristics are also required to accurately model the normal behavior of the system. However, we tried to avoid sensor side feature as long as it would not affect the performance of our IDS significantly. Moreover, agent reports are specially required when the IDS is extended to cover upper layers of the network.

The elements of feature space can further be categorized as statistical features and system specifications. Among different types of IDS, specification-based IDS is more desirable when the system includes a few number of applications and protocols. However, for intrusion detection in physical and data link layer, it is hard to consider some features as system specifications. For example, while average traffic is a key feature in detecting network abnormalities, justifying it as a system specification is difficult, unless for example we assume some kind of industry standard for traffic rate. To avoid such less realistic assumptions we categorize each feature as statistic or specification. While specifications are extracted manually and are not affected by factors such as physical environment, IDS should learn the statistical parameters to adjust its classifier to the environment.

A summary of the feature space is shown in Table 1. The table shows which layer the feature belongs to, and whether it is a specification or statistical parameter. In the following subsections we explain each feature. A brief overview of IEEE 802.15.4 is provided in Appendix A.

4.1.1 Physical Layer Features

P1: Signal strength (Specification, Central IDS): Every node in the network transmits signals with preconfigured power level/levels. Therefore, the strength of the incoming signal in a receiver should be within a specific range. Signals with higher strength than the expected range, might be a result of some malicious activity like jamming. In addition, if sensors use battery as energy source, their signal strength should decrease over time, due to energy consumption. Sudden increase in the power of received signal is an anomalous behavior. For instance the identity of a legitimate node might have been stolen by a powerful malicious node. Our IDS monitors the strength of the received signals over IEEE 802.15.4 frequency band employed by the HAN. Deviations from the normal range can be a sign of malicious activity.

P2: Datagram (Central IDS, Specification): The specifications of the PHY layer datagram, including maximum frame length and reserved bits, are defined for the IDS. Figure 1 shows the structure of a PHY layer frame in IEEE 802.15.4 standard. The length of the physical service data unit varies between 0 to 127 bytes. This length is defined in seven bits of the one byte PHY Header field. The other one bit in PHY header is unused. Our IDS monitors the characteristics of the receiving packet stream and compares them with specifications of a normal frame.

4	1	1	0-127
Preamble	Start of packet Delimiter	PHY Header	PHY Service Data Unit

Figure 1. Structure of PHY frame

P3: Traffic Load (Central IDS, Statistical): During the training phase, IDS measures the average traffic load of each node under normal condition. Using a Gaussian model, a lower and upper threshold for average traffic is defined. Considering that in HAN sensors send their monitored data in a regular basis, deviation from the expected range of traffic load can be due to malicious activity.

P4: Power Consumption Rate (agent, statistical): Sensor nodes have constrained energy. In order to extend the life time, most of the time nodes are in sleep mode. While under normal condition the power consumption rate of a node does not change significantly, an adversary might try to conduct DoS attack by exhausting the node's battery.

4.1.2 MAC Layer Features

M1: Traffic Pattern (Central IDS, Statistical): Three types of data transfer pattern have been defined in the IEEE 802.15.4 standard, including data transfer from a device to the PAN coordinator, data transfer from the PAN coordinator to a device, and data transfer between two peer devices. Each type of transfer can happen in a beacon-enabled or none beacon-enabled network with acknowledged or unacknowledged mode. Deviations from the normal traffic flow can be a sign of malicious activity such as a DoS attack.

M2: Datagram (Central IDS): IEEE 802.15.4 standard defines four MAC layer frame structures. Three of them are transmitted over the network, including:

- Beacon frame for beacon transmission by coordinator.
- Data frame for all kinds of data transmissions.
- Acknowledgment frame for confirming a successful data transmission.

These frame structures are defined for IDS. The IDS in return compares some features of the transmitting frames like frame size and reserved bits to the standard structure, in order to detect anomalous behaviors.

M3: Distribution of Packet Type (Central IDS): In IEEE 802.15.4 several packet types are transmitted over the wireless link. Including, association request/response, GTS request/response, coordinator alignment, data, etc. . Distribution of the network traffic vs. packet types is not uniform. Considering that the main purpose of a sensor network is to sense and report information, data packets should be the dominant type. The distribution of packet types under normal condition is defined for the IDS.

M4: Number of nodes (Central IDS, Specification): Number and identity (ID) of the legitimate nodes are defined for the IDS. When an illegitimate node tries to connect to the network as a new node, the IDS will recognize it as an adversary. We assume that every time a legitimate node is added to the network, for example when a new appliance is added to the HAN, the legitimacy of the node is confirmed by the customer. Although, this can only protect the network from outside attackers.

M5: Packet Collision Rate (Central IDS, Statistical): Packet collision occurs when two nodes try to send packets simultaneously. Since IEEE 802.15.4 has CSMA-CA channel access, under normal condition the collision ratio is low. Abnormal high collision rate might indicate the presence of an adversary. During the training phase the IDS calculates the threshold for maximum collision rate.

M6: Packet Drop Ratio (Agent, Statistical): A packet might be dropped for several reasons. Such as wrong CRC, packet collision, queue fullness, etc. IDS calculates the thresholds for packet drop rate during the training time.

M7: Sequence Number (Central IDS, Specification): The regular ordering of sequence number according to the standard is defined for IDS. Unusual sequence numbers can be suspicious.

Table 1. Elements of feature vector

Layer	Feature	Type
Layer 1	Signal strength	Specification
	Datagram	Specification
	Traffic load	Statistical
	Power consumption ratio	Statistical
Layer 2	Traffic pattern	Statistical
	Datagram	Specification
	Distribution of packet type	Statistical
	Number of nodes	Specification
	Packet collision ratio	Statistical
	Packet drop ratio	Statistical
	Sequence number	Specification

4.2 Classification

Based on the feature vector, the classifier component of the IDS decides whether the system behavior is normal or anomalous. Considering the requirements of HAN explained in Section 3.3, in our IDS we have adopted Bayesian-network classifier [12]. Bayesian-network classifier tries to reduce the number of false positives by defining inter-model dependency and integration of additional data such as confidence level. Bayesian-network classifier consists of a number of models and a root node. Each model is responsible for analyzing one or more features. The model compares the characteristics of the corresponding feature with the pre-established normal properties. According to the degree of deviation from normal properties, each model generates an output. The root node uses model outputs and a threshold value to decide about the system status. For each model a conditional probability table (CPT) is defined. Model looks up the value of the feature in its CPT; the output of the model is the abnormality probability assigned to the given feature value in CPT.

It is possible that two or more models in Bayesian network are correlated. The correlation might be in form of a simple positive or negative effect on the output of another model (an anomalous feature might increase/decrease the probability of another feature being anomalous), or it might be more complex. For instance, the output of one model might indicate that the quality of test for another model is not acceptable. Model dependencies are represented by directed links in network graph. The root node is connected to all models, since its output depends on the output of all other nodes.

A confidence value is assigned to each model, which dictates the influence of the model in root node's decision. Confidence value is the system confidence in the model to generate a correct output. Our IDS assigns a low confidence value to models that experience a high variance over the training period. On the other hand, we assign higher confidence value to models which their anomalous behavior is less expected under normal condition. In other words, we use confidence value as the weight of model; this weight can dynamically change according to training environment. For each model we define a CFP either based on specification of the feature or threshold values learnt in training phase. While thresholds of statistical parameters are calculated by model during the training time, the conditional probabilities are fixed values. We define the conditional probabilities and confidence values based on our previous knowledge.

Figure 2 depicts the structure of the Bayesian-network classifier that we have designed in our IDS. As it is shown in the figure, our Bayesian-network comprises the following model dependencies:

Singal strength – collision: The intuition behind this correlation is that receiving a high power signal in IEEE 802.15.4 frequency band, might be due to the existence of another legitimate network rather than a malicious activity. For example, 802.11 WLAN might work in the same frequency band as IEEE 802.15.4. Therefore, unless the IDS detects an anomalous collision, rate the signal strength model does not declare anomaly.

Power consumption – traffic load: Not only power consumption above an appropriate threshold is peculiar, constant power consumption ratio while the traffic load is higher than normal is also anomalous. This can be due to the existence of an adversary node injecting traffic to the network using spoofed ID of legitimate nodes.

Traffic load – distribution of packet type: Higher than usual traffic load is more unexpected when the distribution of packet is anomalous. For example while some degree of change in traffic load for data packet is acceptable signals like GTS deallocation are not expected to be sent in high volume.

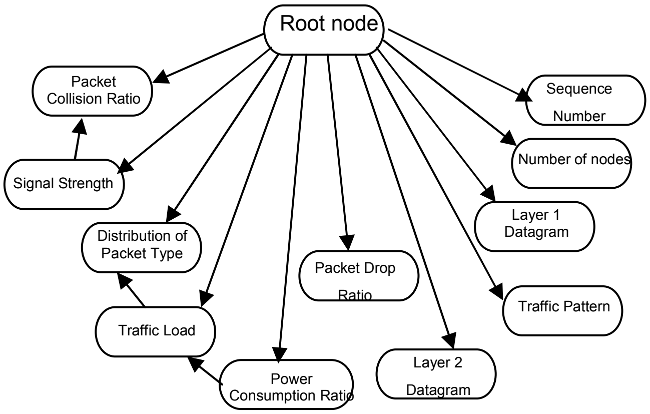

Figure 2. Structure of Bayesian network classifier

5. IEEE 802.15.4 Attacks

In this section a number of known attacks against IEEE 802.15.4 are introduced breifly. We use these attacks in the following section to evaluate the functionality of our proposed IDS.

5.1 Radio Jamming

Radio jamming is an intentional or unintentional emission of radio signals that interfere with the information flow of a wireless network, which can lead to the disruption of the communication by decreasing the signal to noise ratio. An attacker can deliberately use radio jamming to cause denial of service. In [19], three types of radio jamming attacks against 802.15.4 are implemented in hardware including:

Wide-Band Denial: In this method, the whole RF spectrum is blocked by transmission of jamming signals with high power over the related frequency band. This is the simplest form of jamming. However, it can easily be detected, and the power consumption of the attacking node is relatively high.

Pulse Denial: In this type of jamming, instead of continuous transmission of the jamming signal over a wide frequency band, jamming signals are emitted in form of pulse signals with short time periods on each channel. Using channel-hopping over all IEEE 802.15.4 channels, pulse jamming can cause a wide-band denial.

IEEE 802.15.4 Specific Interruption Denial: The attacker listens to the wireless traffic and whenever it detects 802.15.4 traffic it starts to transmit jamming signals. In this way the jamming will not affect other networks that use the same frequency band (WiFi in 2.4GHz band for instance). The fact that the interfering transmitter does not work continuously, makes the detection of this attack harder compare to previous jamming types.

5.2 GTS Attacks

According to the IEEE 802.15.4 standard the PAN coordinator can allot some of the superframe slots called GTS to a specific node. This can be helpful for applications that need a specific bandwidth or low latency. In [20] four IEEE 802.15.4 MAC layer attacks are introduced. All of these attacks are designed based on the misuse of GTS management scheme.

DoS against data transmission during contention free period (CFP): In this attack a malicious node that is located in the transmission range of the PAN coordinator spoofs the IDs of legitimate nodes, eavesdrops network traffic to extract information such as the number of legitimate nodes in the PAN, and the requests and usage of the GTSs by legitimate nodes. Then the malicious node sends GTS deallocation requests to the PAN coordinator and terminates the data flow of legitimate nodes.

DoS against GTS requests: An adversary node keeps track of the GTS list and tries to fill up all of the available GTS slots by sending several GTS allocation requests. In this way, legitimate nodes will not find the chance to transmit their data during the CFP. This is an energy efficient attack, since the attacker does not send any data other than allocation requests.

Stealing network bandwidth: In this attack, the malicious node tries to occupy all of the GTS slots by sending GTS allocation requests. But this time the attacker also transmits data packages during the allocated time slots, so that the coordinator does not drop the allocated time slots. This attack not only exhausts the bandwidth and disturbs the flow of legitimate traffic, but also prevents the PAN coordinator to go to the sleep mode.

Another type of GTS attack is introduced in [21]. A malicious node listens to the network traffic and monitors the GTS allocated slots. It then creates interference signals during the allocated slots to corrupt the data packets. This attack can be considered as a layer two jamming.

5.3 Back-off manipulation

This attack was originally introduced for IEEE 802.11 distribution coordination function (DCF). Since IEEE 802.15.4 standard uses a similar CSMA based protocol, it is also applicable for this standard [22]. In DCF when a node wants to transfer a packet, it first listens to the channel in order to make sure that the channel is free. If the channel is busy, it will wait for a “back-off period” and then tries again. The duration of the “back-off period” is chosen randomly in a specific range. Each time a node encounters to a busy channel this range increases exponentially. A malicious node can steal channel access of the legitimate nodes, by circumventing the protocol rules and using an instantly short back-off period.

5.4 Replay-protection attack

IEEE 802.15.4 uses a replay-protection mechanism in which the sequence number (SN) of the received frame is compared with the SN of the previously received frame. If the SN of the former is equal or smaller than the SN of the latter this frame will be dropped. An attacker might send frames with large SN to a receiver. Receiver then will drop the legitimate packets due to their smaller SN [23].

5.5 Steganography attack

Steganography means embedding a secret message into another media. In communications, one can use the reserved or unused fields of a network protocol to transfer hidden data. It is possible to create hidden channels by use of this attack. A detailed investigation on steganography attacks in IEEE 802.15.4 is reported in [24].

6. EVALUATION

In order to evaluate the performance of our proposed IDS, we simulated a ZigBee network in NS-2 simulation environment. Since the existing versions of NS-2 does not support GTS mechanism of IEEE 802.15.4 we employed the GTS implementation provided in [27]. We made several other changes in the source code of WPAN package to facilitate the implementation of our attack scenarios.

Simulation parameters are shown in Table 2. We established a network with star topology consist of 17 ZigBee nodes, one FFD node as the private area network (PAN) coordinator, and 16 RFD nodes as sensor devices. We used one of the RFD nodes as adversary. Five nodes work in GTS mode. The traffic type is CBR; legitimate sensor nodes send data packets in five seconds time interval, and the coordinator sends data packets to sensor nodes every one minute.

Table 2. Simulation Parameters

Parameter	Value
NS-2 version	2.34
Routing Protocol	DumbAgent
Simulation Area	50mx50m
Traffic	CBR
Beacon	Enabled
Beacon Order	3
Superframe Order	3

6.1 Training Phase

In training phase we run the simulation for 10000 seconds, under normal condition. During this time all nodes including the adversary operate properly. We used the simulation results to find the CPT threshold values of statistical features. The IDS keeps a record of CPT tables for each node. Table 3 shows CPT for traffic load, as one example of CPT table. The parameters are measured in 300 seconds time frames. The IDS uses the same time window in detection mode, meaning that detection time can be delayed up to 5 minutes. By changing this value one can make a trade off between detection delay and network overhead. We emphasis that conditional probabilities are not adjusted according to training data. These values are defined manually based on expert-domain knowledge. We assigned the confidence value of *3* to datagram model since it is very unusual for a reserved bit to vary without affecting the value of Cyclic Redundancy Check (CRC). The same value is assigned to the confidence value of sequence number model. The confidence value of all other models, are *1*. The total output of the classifier is the summation of the output of each model weighted by their confidence level. The threshold value of the output is *2*.

Table 3. CPT for traffic load

feature value (packet/5min)	distribution of packet type <0.5	distribution of packet type >0.5
<20	0.5	0.7
20< <55	0.3	0.5
55< <95	0	0
95<	0.6	0.9

6.2 Testing Phase

We simulated the three of the attack types introduced in Section 5 to evaluate the detection capability of our IDS.

Back-off manipulation attack: To implement the back-off manipulation attack, we decrease the CSMA-CA waiting time, *wtime*, of the adversary node by factor of *k*. When the adversary encounters a busy channel, instead of *wtime* it waits for *wtime/k*. Figure 3 shows the impact of *k* on the average traffic load and number of dropped packets of a legitimate (non GTS) node.

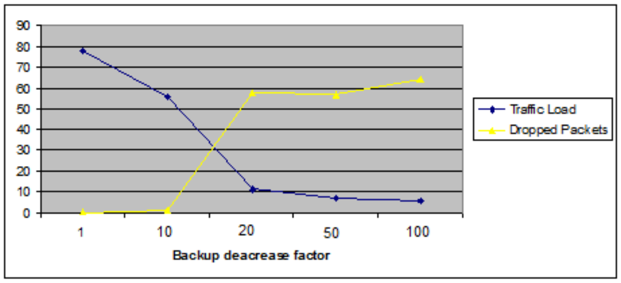

Figure 3. Effect of incorrect waiting time. (Traffic Load: number of packets per 5min, Dropped Packets: number of dropped packets per 5min.)

*DoS against GTS request***:** To simulate this attack we mended the GTS code to allow adversary to send GTS deallocation requests with spoofed ID of legitimate nodes available in GTS list. The adversary then sends GTS allocation requests to the coordinator, to fill up all GTS slots. In original attack the adversary just listens to the beacon frame and fills the free GTS slots, then it waits for other nodes in the list to deallocate the occupied slots. As soon as one GTS is free, the adversary fills the slot by sending a GTS request. We made this modification since in our scenario the GTS nodes never send deallocation requests. In current implementation of GTS when a GTS node fails to get a GTS slot, it does not switch to the CAP, therefore its data traffic load reduces to zero.

DoS against data transmission during CFP: We modified the GTS code to allow the attacker to read the GTS list. The adversary then sends GTS deallocation with spoofed ID of nodes in the GTS list. In addition, whenever the adversary hears a GTS allocation request, it sends a deallocation request on behalf of legitimate node.

The IDS was successful to detect variations of the above attacks in addition to Steganography attack. Table 4 shows which models are triggered for each attack. However, we have not yet simulated scenarios that can challenge the IDS performance in resisting false positives. One possible scenario could be a WiFi network in the vicinity of a ZigBee network. WiFi works at the same frequency range and has higher signal strength.

Table 4. Proposed IDS against some IEEE 802.15.4 attacks

Attack	Detection Potential	Specification
Wide-band denial	√	P1, P4, M3, M5, M6
Pulse denial	√	P1, P4, M3, M5, M6
802.15.4 specific interruption	√	P1, P4, M3, M5, M6
DoS against data trans. In CFP	√	P3, M3
DoS against GTS requests	√	P3, P4, M4, M6
Stealing network bandwidth	√	P3, P4, M3, M6
Back-off manipulation	√	P3, P4, M6
Replay-protection	√	M7
Steganography	√	P2, M2

7. DISCUSSION

Estimating appropriate values for CPT probabilities require a deep knowledge and experience in field of wireless network and specifically IEEE 802.15.4 standard. We are not expert in this domain and we do not claim that the parameters we used in our Bayesian network are optimum. Also the structure of present Bayesian network can be improved by designing more accurate relationships between models as well as adding/removing some features.

We tried to evaluate the performance of the proposed method through simulation. Our IDS has the potential to detect most of the existing attacks and since the IDS is based on anomalous event detection, we expect the same for unknown attacks. However, our data set was not extensive enough to provide thorough quantitative performance analysis. We believe that providing appropriate databases for public access will accelerate the progress in the critical area of IDS.

Still we believe that the proposed IDS scheme, especially in the context of HAN, is superior to many other IDS approaches. Some advantages of this method include:

- It does not require any knowledge of attacks.
- By accurate adjustment of IDS parameters, a low false positive rate is achievable.
- It has a very low computational and network overhead.
- Unlike many machine learning approaches the classification result is a real number, which allow the dynamic assignment of threshold for distinguishing anomaly and normal events.

8. CONCLUSION

In this work we addressed the problem of intrusion detection in future HAN as a subnetwork within the smart grid. We reviewed the security challenges in HAN, and investigated the requirements of IDS in such a network. According to characteristics and limitations of HAN, we proposed a Bayesian network intrusion detection system tailored for IEEE 802.15.4, as the dominant standard in future HAN. We overviewed the existing attacks against IEEE 802.15.4 standard and through simulation evaluated the performance of our IDS against them. Simulation results showed promising detection capability for the proposed approach. Still a larger data set is required to provide strong quantitative performance measurements. In the future, we plan to provide a larger data set to evaluate the performance of our IDS. Further, we will extend our IDS to cover the upper layers of ZigBee technology.

9. REFERENCES

[1] Testimony before the house committee on homeland security subcommittee on emerging threats, cybersecurity, and science and technology, United States House of Representatives (July 21, 2009, 4) (Testimony of Cita M. Furlani, Director, Information Technology Laboratory)

[2] NISTIR Guidelines for smart grid cyber security v1.0 – Aug 2010.

[3] N. Kush, F. Ernest, E. Ahmed, I. Ahmed, and A.Clark. Gap analysis of intrusion detection in smart grids. In *Proceedings of the 2nd International Cyber Resilience Conferenc*e, August 2011.

[4] L. Wang, W. Sun, R.C. Green, M. Alam. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. *IEEE Transaction on Smart Grid*, vol. 2, no. 4, pp. 796-808 , Dec. 2011.

[5] R. Berthier, W.H. Sanders, H. Khurana. Intrusion detection for advanced metering infrastructures: requirements and architectural directions,*first IEEE international Conference on smart grid communications,* Oct. 2010.

[6] T. Roosta, D.K. Nilsson, U. Lindqvist, A. Valdes. An intrusion detection system for wireless process control systems, *5th IEEE international conference on mobile Ad Hoc and sensor systems*, Oct. 2008.

[7] V.B. Misic, J. Begum . Evaluating the feasibility of traffic-based intrusion detection in an 802.15.4 sensor cluster, *21st international conference on dvanced information networking and applications*, 21-23 May 2007.

[8] A.S. Mohammad, Z. Mohammad, Efficiency of Markov Models Over Neural Networks in Anomaly Intrusion Detection, In *30th Annual International Computer Software and Applications Conference*, 2006

[9] M. Crosbie and E. Spafford. Applying Genetic Programming to Intrusion Detection, In *Proceedings of the First Annual Conference on Genetic Programming*, 1996.

[10] K. Ilgun, R. A. Kemmerer, P. A. Porras. State transition analysis: a rul based intrusion detection approach. *IEEE Transaction on Software Engineering, vol. 21, pp. 181-199,* 1995

[11] S. Forrest, S. A. Hofmeyr, A. Somayaji. Intrusion detection using sequences of system calls. *journal of Computer Security* vol. 6, pp. 151-180, 1998.

[12] C. Kruegel, D. Mutz, W. Robertson, F. Valeur. Bayesian event classification for intrusion detection. *Proceeding of 19th Annual Computer Security Applications Conference*, Dec. 2003.

[13] A. El-semary, J. Edmonds, J. Gonzalez, M. Papa. A framework for an adaptive intrusion detection system. *in The 14th IEEE International Cinference on Fuzzy Systems,* 2005, pp 325-330.

[14] T. Abbes, A. Bouhoula, M. Rusinowitch, Protocol analysis in intrusion detection using decision tree. *In Proceeding of International Conference on Information Technology, Coding and Computing*, 2004

[15] http://www.smartgridelectronics.net/2010/12/ge-study-found-ZigBee better-than-wifi-for-smart-grid/

[16] K. scarfone, P. Mell. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, NIST (National Institute of Standards and Technology) special publication 800-94, 2007.

[17] S. Axelsson. The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information and System Security*, vol. 3, no. 3, 2000.

[18] S. Robin, P. Vern, Outside the closed world: on using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 2010.

[19] C.P. O'Flynn. Message denial and alteration on IEEE 802.15.4 low-power radio networks. *4th IFIP International Conference on New Technologies, Mobility and Security*, Feb. 2011.

[20] R. Sokullu, O. Dagdeviren, I. Korkmaz. On the IEEE 802.15.4 MAC layer attacks: GTS attack. *Second international conference on sensor technologies and applications*, Aug. 2008.

[21] Y.W. Law, P. Hartel, J. den Hartog and P. Havinga. Link-layer jamming attacks on S-MAC", in *Proceedings of IEEE Wireless Sensor Network*, 2005.

[22] S. Radosavac, A. A. Crdenas, J. S. Baras and G. V. Moustakides. Detecting IEEE 802.11 MAC layer misbehavior in Ad Hoc networks: robust strategies against individual and colluding attackers. *Journal of Computer Security, special Issue on Security of Ad Hoc and Sensor Networks*, vol.15, 2007, pp.103-128.

[23] Y. Xiao, S. Sethi, H. Chen, B. Sun. Security services and enhancements in the IEEE 802.15.4 wireless sensor networks. In *Proceedings of IEEE GLOBECOM'05*, vol.3, 2005.

[24] D. Martins, H. Guyennet. Attacks with steganography in PHY and MAC layers of 802.15.4 protocol. *5th International Conference on Systems and Networks Communications*, Aug. 2010.

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

[26] A. Patcha, J.M. Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *The International Journal of Computer and Telecommunications Networking*, vol. 51. no. 12, Aug. 2007.

[27] W. Choi, S Lee. Implementation of the IEEE 802.15.4 module with CFP in NS-2. *Telcommunication Systems. DOI 10.1007/s11235-011-9548-7,* Aug. 2011.

Appenix 1

Zigbee is a low power consumption, low data rate, low cost wireless technology which was originally designed by Zigbee Alliance for use in automation and remote control applications. A short while later IEEE 802.15.4 committee started to work on a low data rate, low power consumption standard as well. These two groups later joined their forces to develop a single technology under the commercial name of Zigbee

IEEE 802.15.4 focuses on the physical and data link layer protocols. Some characteristics of this standard include:

- CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) channel access.
- Star or peer-to-peer network topologies
- Allocation of Guarantied Time Slots (GTS)
- Reliable transfer through fully acknowledge protocol
- 16 channels in the 2450MHZ band, 10 channels in the 915MHz band, and 1 channel in the 868MHz band.

An IEEE 802.15.4 system might contain three types of devices. Full Function Device (FFD) is a node with full functionality including data send/receive and routing. Reduced Function Device (RFD) is a simpler node with limited functionality. An RFD can only talk to an FFD and it does not support routing. A Coordinator is a special form of FFD with some extra capabilities. This node is responsible for control of the network.

An IEEE 802.15.4 network can operate in either nonbeacon-enabled or beacon-enabled modes. In the former data frames are simply transmitted using unslotted CSMA-CA, while in the latter data is transmitted in superframes. Beacon frame is the first slot of each superframe and is responsible for synchronizing the network devices, identifying the PAN, and describing the structure of the superframe. GTS slots are part of the superframe that are used for collision free transmission. GTS slots are transmitted during contention free period (CFP) while other slots are transmitted during contention access period (CAP).

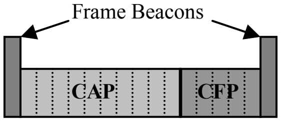

Figure A1. Superframe structure