A Novel Intrusion Detection Framework for Wireless Sensor Networks

Murad A. Rassam, Mohd. Aizaini Maarof, and Anazida Zainal
Department of Computer Communications and Systems
Faculty of Computer Science and Information Systems,
Universiti Teknologi Malaysia,
81310, Skudai, Johor, Malaysia.
murad.utm@gmail.com, anazida, aizaini @utm.my

***Abstract*—Wireless Sensor Networks (WSN) security issues are getting more attention by researchers due to deployment circumstances. They are usually deployed in unattended and harsh environments that make them susceptible for many kinds of attacks. Different security mechanisms have been proposed for WSN. Detection-based mechanisms are considered to be the second defense line against attacks when the traditional prevention based mechanisms failed to detect them. Different intrusion detection schemes have been introduced (e.g. rule based, statistical based…etc). Rule-based intrusion detection schemes are considered to be the fast and simple schemes that are suitable for the demand of WSN. However, these schemes are more specific to some kinds of attacks and cannot be generalized. In addition, these schemes cannot detect the unknown attacks that are not included in their rule base. In this paper, we highlight the limitations of the state-of-the-art rule based intrusion detection schemes and then introduce a novel framework based on rule based scheme that is able to overcome these limitations.**

Keywords-Wireless Sensor Networks; Security; Intrusion Detection; Rule Learning;

I. INTRODUCTION

Wireless Sensor Networks are kind of networks that formed by hundreds to thousands of tiny resource constrained devices called sensors[1]. WSNs are categorized into two main categories based on their application areas: monitoring and tracking. Each category is further categorized to sub-categories; i.e. monitoring the environment, habitat, health, and battlefield [2]. The fact that WSNs are deployed in harsh environments and are resource constrained in terms of power, storage, and processing makes them vulnerable to different types of attacks; i.e. DoS, Wormhole, Sinkhole attacks,etc.

Attacks on WSN are classified into two main categories based on the source of attacks: insider attacks, and outsider attacks[3]. Insider attacks are attacks that are launched by compromised nodes that belong to the network; whereas outsider attacks are launched by outsider parties like laptop-class attacks which is initiated from outside the network using high performance devices i.e. laptops [3]. To protect WSNs against the broad range of attacks, prevention-based security solutions like cryptography, authentication, and key management have been introduced. Although these mechanisms are considered the first defense line against attacks, they are only effective to protect from certain kinds of outsider attacks and failed to protect the network from insider attacks[3, 4]. Because of that, there was a need for another layer of protection.

Intrusion Detection Systems (IDS) have been used as a second defense line against intruders in many types of networks. However, their use in WSN poses many challenges due to constraint resources [4]. IDS for WSN can be categorized into 4 schemes and they are: rule-based, statistical based, game theoretical based, and data mining & computational intelligence based schemes. Each scheme has its advantages over the others as well as its drawbacks.

Rule-based IDS scheme also called specification based IDS and it is the most common IDS scheme that is proposed for WSN. There are three fundamental phases of the scheme: data acquisition, rule construction by domain expert, and the intrusion detection [4]. Rule-based schemes are suitable for WSN because they are simple to be implemented and fit the demands of WSN resources restriction. However, most of the current rule-based schemes are attack specific, therefore cannot detect a broad variety of attacks. In addition, they cannot cope with novel attacks as their rules are already created for specific types.

This paper proposes a novel framework that aims to overcome the drawbacks of rule based IDS in WSNs. In this framework, two main concepts are introduced; smart rule construction is aimed to address the generality issue to detect as much as possible of known attacks. The second is rule learning in which the new emerging attacks are learned continuously by a simple learner.

The rest of this paper is organized as follows: Section II describes some related works. In section III, the proposed framework is introduced, and finally this paper is concluded in Section IV.

II. RELATED WORKS

A decentralized intrusion detection system in WSN has been proposed by Silva [4] as a first rule based IDS scheme for detection of many different kinds of attacks in different WSN layers. In this scheme, there are three main phases: data acquisition performed by monitor nodes that promiscuously listen to the messages and filter the information needed for analysis and design of the rules. Then, the rules are constructed based on the information extracted in the previous phase. Finally, the intrusion detection phase is performed based on the application of the

978-1-4577-2155-7/11/$26.00 ©2011 IEEE

rules and the comparison of the errors raised by the monitor nodes. Although this scheme brings a good framework to the rule based IDS for WSN, it has some drawbacks. The procedure in determining the number of monitor nodes which will be involved in the IDS is unclear. Besides, it is limited to specific types of attacks that make it unable to detect new emerging attacks.

Pires et al.[5] introduced a scheme based on the received signal strength measured in each node to identify the possible malicious node. This scheme is specific to two types of attacks which are HELLO flood and wormhole attacks in WSN. Its mechanism is based on the comparison of energy of the received signal and the energy of the same observed signal around the network. In addition to the restriction to two attacks, the signal strength may be affected by other reasons, such as channel collision, and interference.

An intrusion detection system against node impersonation attack and resource depletion attacks has been proposed by Onat and Miri [5]. In this scheme, two features are used, to build a statistical profile of the neighborhood behavior, which are the received power rate and the arrival packet rate. The specificity of detection only on two types of attacks and the possibility of other factors like operation errors of sensors affect the features are the main drawbacks of this scheme.

Krontiris et al.[6] Introduced a lightweight intrusion detections scheme for detecting selective forwarding and blackhole attacks in WSN. In this scheme, the nodes monitor their neighbors and collaborate to decide if there is a possible malicious node or an intrusion has taken place. To minimize the computation overhead, the task of deciding on occurrence of attacks is divided on all nodes instead of few monitoring nodes. Similar to other rule-based schemes, they are limited to specific attacks.

Another intrusion detection scheme has been proposed by Krontiris et al.[7] to detect sinkhole attack in WSN. In this scheme there are four modules: Local Packet Monitoring Module, Local Detection Engine Module, Cooperative Detection Engine, and Local Response Model. MintRoute protocol was used as the based routing protocol implemented in TinyOS environment. On the other hand, this scheme implements the distribution of work which is highly required in a large scale and autonomous environment like WSN.

Another scheme that is based on the collaboration between neighbors has been presented by Stetsko [8] for detection of three kinds of attacks: HELLO flood, selective forwarding, and Jamming attacks. This scheme is implemented on the Collaboration Tree Protocol (CTP) on the TinyOS environment using two features: packet sending rate and packet dropping rate. In addition, to the limited scope of detected attack is another drawback of this scheme.

The high communication overhead caused by the collaboration between nodes is a common feature in schemes [7-9]. Knowing that, the communication overhead is often several orders of magnitude higher than the computation overhead [1], this drawback is very critical for WSN.

A fuzzy rule based intrusion detection scheme for directed diffusion based WSN has been introduced by Chi and Cho [9]. Traffic features such as node energy level, message transmission rate, neighbor node list, and error transmission rate are extracted to build the fuzzy rules. This scheme is dedicated for detection of Denial of Service (Dos) attacks which always drain the resources of the WSN. The four features mentioned are used by the fuzzy controller and applied on the traffic collected in the base station or in monitoring nodes. The selection procedure on quantity & type of monitoring nodes to protect the network are unclear. This approach is highly depends on expert to design the rules for every known attack. The manual creation of rules makes the system rigid and cannot cope with novel attacks which are not included in the rule set.

Another fuzzy logic based intrusion detection scheme to detect sinkhole attack in directed diffusion WSN has been introduced in [10]. Two features are used which are the reinforcement ration and the radius are used by the fuzzy controller as an input to decide on the detection value which is the output. Prior the application of the fuzzy rule based scheme, fuzzy rules need to be prepared by an expert and this is the main drawback of this kind of schemes that make them inflexible and limit their scopes for some kinds of attacks. Similar scheme based on fuzzy logic proposed by ponomarchuk and Seo [11]. Two main features which are the packet reception rate and the packet inter-arrival time were used in a time window. This scheme has the same drawbacks like other rule based schemes which is the dependency on the expert knowledge to build the rules.

Recently, Sousa Lemos [12] has proposed a collaborative IDS scheme to detect node repetition attack in WSN. Some nodes in this scheme are chosen to act as monitor nodes to monitor the behavior of the rest nodes based on some defined rules. Another type of nodes called supervisor nodes are used and they are responsible for correlating the decisions made by the monitoring nodes. The main advantage of this scheme is that, it provides layers of protection by using these two types of nodes, but unfortunately monitor & supervisor nodes could be a point of failure to the network if they got compromised. Usually, most of researchers assume that those nodes are protected from any kind of failure but this assumption is not always true for many WSN applications.

Rule based intrusion detection schemes has some advantages over other schemes which are based on different techniques like statistical, game theoretical, and data mining techniques. These schemes are characterized by fast detection feature because there is no training here and the detection agent does not need to learn both normal and abnormal profiles. This feature is useful in some WSN online applications that have a continuous streaming data. Besides, rule based IDS has low computational complexity since they are based on some predefined rules. In these schemes, detection accuracy is heavily dependent on quality of rules.

Despite the mentioned advantages of the rule based schemes, they also have some drawbacks. The detection generality is the main drawback that characterizes these schemes since they are designed to detect specific kinds of attacks. Another drawback is the high communication overhead when it involves voting in determining the occurrence of attack. Furthermore, most of the rule based schemes made many assumptions that limit the scopes of and restrict to certain WSN applications. The use of different metrics to measure the effectiveness of the scheme implies the absence of mature standards that are usually used in other paradigms.

To conclude, there is a need to develop rule based schemes that emphasizes on the advantages mentioned above and overcome the limitations. This paper introduces a framework that addresses the issue of detection generality by incorporating the rule learning at the base station. In the following section, the proposed framework is introduced.

III. A NOVEL RULE BASED INTRUSION DETECTION FRAMEWORK FOR WSN

Figure 1 shows the proposed rule based intrusion detection framework. A brief explanation about its phases is followed. The scheme is composed of three main phases: the preprocessing, the general rule construction, and the rule learning.

A. Phase1: Preprocessing

This phase is composed of some process in which the data is collected and prepared for the rules construction in the second phase. After setup the sensors and build the WSN structure, the data will be collected from the sensor nodes by the base station through multi-hop routing process. The network will be setup to perform the collection of temperature, humidity, and light from the place of deployment. After collecting the normal data through the normal activities of the network, some types of attacks will be launched through specific sensor nodes and the data affected by the malicious activities will be collected too.

During the collection of the data from normal and abnormal activities, the focus should be pointed towards the features that change their values because of such type of attacks. These features will differ from routing protocol to another. The feature selection process means that specific features that are affected by the malicious node activities and for different types of attacks should be given the higher priority in selection compared to the features that keep out of change. By the end we will get the most important features that will help in differentiating between normal activity and attack. By the end of this phase, we get the features that help us in building the rules.

B. Phase2: Rules Construction

This phase is composed of some sub-phases as follow:

Smart and Generic Rules Construction: in this sub-case and based on the features extracted from the previous phase, the expert and based on some experience about the features that always affected by a specific type of attack will design and construct the required rules needed to detect that attack. The meaning of the smart rule is that the rule should be able to act in place of some other rules. It means, if we have two or three rules that are responsible to detect an attack, if we can construct only one rule that could do the work of all of them we call that rule a smart rule. The use of smart rule is very important to avoid the growth of rules. The meaning of the generic rule is that the rule should be built in a way that it could identify or detect many attacks. Some of attacks always change common features so generic rules could be designed to detect them all. The use of smart and general rules will help in keeping the number of rules a minimum and therefore minimize the power consumption in the network.

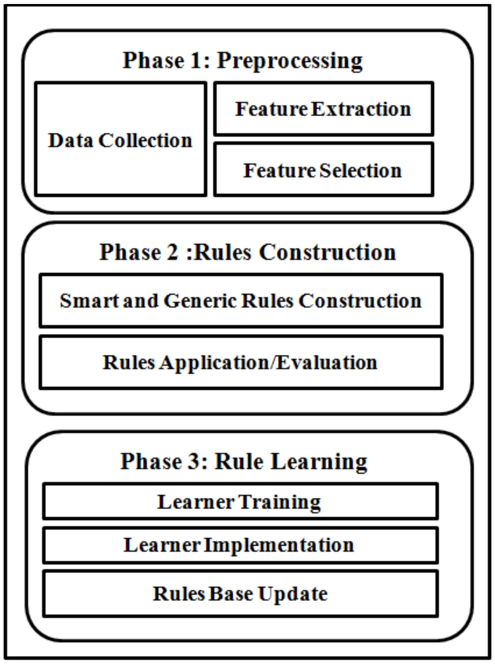

Figure 1: The General Proposed Framework

Rules Application: means after the rules are ready, they will be applied on the network traffic. This is an online process whereas the previous ones (data preprocessing and rules construction) will be done offline.

Rules Matching/Evaluation: in this process and after applying the rules on the traffic, the rules are checked if there is a deviation in the traffic from the normal behavior. Based on that, an alarm along with the node id should be raised to the administrator which is the base station in our case to inform about the attack. If there is no deviation, the data will be forwarded as usual to the base station in a multi-hop fashion.

C. Phase3: Rule Learning

This phase is also composed of three main sub-phases which are the learner training, learner implementation, and the update of rules.

Learner Training: in this sub-phase, a suitable machine learning technique will be used for rule learning. This technique will be first trained offline to learn the rules of the known attacks. After that, an incremental learning will be involved to learn the new unknown attacks that emerge continuously. It should be known that for each type of attacks there are specific features used to detect them. It is also important to know that the rule learning is required to learn the new attacks for the future retection. These new attacks will be blocked from any further damage when they violate the predefined rules of known attacks. The learning process will be done to generate new rules for the future attacks from that kind and not for the attacks in real time.

Learner Implementation: after train the learner, it should be able to generate new rules for that new specific attack.

Rules Update: in this sub-phase, the new generated rules will be sent back to the sensor nodes to update their rule bases for detection of the new attacks learned by the rule learner.

IV. CONCLUSION AND FUTURE WORK

As different kinds of attacks are emerging continuously, security becomes a hot issue for WSN because of their deployment circumstances and their resource constraints. Although, a variety of security mechanisms have been introduced to protect these kinds of networks, these mechanisms still not able to protect them. Intrusion detection schemes are considered to be the second defense line against the insider attacks that are caused by the compromised nodes from inside the network itself. In this paper, a novel intrusion detection framework has been introduced showing its potential improvements and its ability to overcome the drawbacks of the rule based intrusion detection schemes. Two main points have been emphasized: the smart and general rule construction, and the rules learning. We expect that this framework will advance the design of a suitable lightweight intrusion detection system for a variety of WSN applications. This work is exploratory in which many experiments will be conducted to verify the viability of the framework.

ACKNOWLEDGMENT

This work is supported by the Ministry of Higher Education (MOHE) and Research Management Centre (RMC) at Universiti Teknologi Malaysia (UTM) under FRGS Grant (VOTE NO. 77218).

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks,* vol. 38, pp. 393-422, 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks,* vol. 52, pp. 2292-2330, 2008.

[3] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials,* vol. 8, pp. 2-23, 2006.

[4] A. P. R. d. Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," Montreal, Quebec, Canada, 2005, pp. 16-23.

[5] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *IEEE International Conference on, Wireless And Mobile Computing, Networking And Communications, (WiMob'2005)*, 2005, pp. 253-259 Vol. 3-253-259 Vol. 3.

[6] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," *In Proc. of the 13th European Wireless Conference,* 2007.

[7] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," Wro&caw, Poland, 2008, pp. 150-161.

[8] A. Stetsko, L. Folkman, and V. Matyáš, "Neighbor-Based Intrusion Detection for Wireless Sensor Networks," in *International Conference onWireless and Mobile Communications* Los Alamitos, CA, USA, 2010, pp. 420-425.

[9] S. H. Chi and T. H. Cho, "Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks," in *Fuzzy Systems and Knowledge Discovery*. vol. 4223, L. Wang*, et al.*, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 725-734.

[10] S. Y. Moon and T. H. Cho, "Intrusion Detection Scheme against Sinkhole Attacks in Directed Diffusion Based Sensor Networks," *International Journal of Computer Science and Network Security,* vol. 9, 2009.

[11] Y. a. S. Ponomarchuk, DW., "Intrusion Detection based on Traffic Analysis and Fuzzy Inference System in Wireless Sensor Networks," *Journal of Convergence,* vol. 1, December 2010 2010.

[12] M. V. Sousa Lemos, L. B. Leal, and R. H. Filho, "A New Collaborative Approach for Intrusion Detection System on Wireless Sensor Networks," in *Novel Algorithms and Techniques in Telecommunications and Networking*, T. Sobh*, et al.*, Eds., ed Dordrecht: Springer Netherlands, 2010, pp. 239-244.