Packet Flow Rate to Protect Wireless Sensor Networks from Wormhole and Hello Flood Attacks

HosamSoleman
Department of ComputerEngineering
Maleke-Ashtar University
Islamic Republic of Iran

Ali Payandeh
Department of Computer Engineering
Maleke-Ashtar University
Islamic Republic of Iran

Nasser Mozayyani
School of Electrical & ComputerEngineering
Elm-o-Sanat University Islamic Republic of Iran

Saeed Sedighian Kashi
School of Electrical & ComputerEngineering
K. N. Toosi University of Technology

ABSTRACT

The increased deployment of ubiquitous wireless sensor (WSN) networks has exponentially increased the complexity to detect wireless sensor network attacks and protect against them. Wormhole and hello flood attacks can destabilize or disable wireless sensor networks. In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wired or wireless link with less latency than the network links, and relays them to another point in the network. Hello flood attack is an important attack on the network layer, in which an adversary, which is not a legal node in the network, can flood hello request to any legitimate node using high transmission power and break the security of WSNs. This paper describes detection algorithms for wireless sensor networks, which detects wormholes and hello flood attacks based on the packet flow rate to base station node in the network. Simulation results show that the algorithms have low false toleration and false detection rates and small time to detect attacks.

Keywords:

Wireless sensor network, packet flow, cluster topology, wormhole attack, hello flood attack.

1. INTRODUCTION

Wireless sensor networks are composed of many lowcost micro sensor nodes which are deployed in the monitoring area. Each sensor node can form a multi-hop self-organizing network through wireless communication, and each sensor node is capable of sensing, data processing and communication [1]. Generally speaking, wireless sensor network is often deployed in an open environment, even the enemy-occupied domain. As sensor nodes transfer data through wireless communication link, the network can be easily captured and invaded. Due to the lack of foundation infrastructure like wired network, what wireless sensor networks face not only traditional security threats but also some attacks which include the exhaustion attack, selective forwarding-attack, wormhole-attack, sinkhole-attack, Sybil attack, hello-flood-attack, etc… Besides, each sensor node has limited energy and processing capability, small storage capacity and low bandwidth, this put forwards a larger challenge for the security of wireless network.

The objectives of our algorithms are to detect wireless sensor network attacks and generate counter measures to protect the WSN and the privacy of the users. The algorithms areusingpacket flow rate that arriving to base station from cluster headers of network. Wireless sensor network flows (WSNetFlow) are learned and mined to select the features that are most relevant to different types of normal traffic and attack.

In this work, we focus on two types of attacks: HELLO flood attacks [2] and wormhole attacks [3]. HELLO messages are used in many protocols by nodes that want to announce their presence and proximity to their neighbors. Most of these protocols rely on the assumption that a node A is within the radio transmission range of another node B if A is able to receive messages from B. In a HELLO flood attack, a malicious

node may try to transmit a message with an abnormally high power so as to make all nodes believe that it is their neighbor.

Wormhole attacks can be described in the following steps. An adversary A tunnels a message received to a second adversary B in a distant part of the network using a lowlatency out-of-band channel. B then retransmits the message exactly as received to the nodes in its neighborhood.

An immediate result of a wormhole attack is that nodes that hear the transmission from B are tricked into thinking that they are neighbors of whichever node originated the message (this node is most likely located in a distant part of the network).

Both the HELLO flood attack and the wormhole attack are typically carried out to compromise route establishment in a network. For example, a malicious node that broadcasts a routing beacon with an extra high power could lead a large number of nodes to attempt to use it as their next hop in their route to the sink. But those sufficiently far away would be simply sending their messages into the oblivion. A similar scenario results from a wormhole attack. A malicious node could convince nodes that are normally multiple hops from the sink node that they are just one hop away. These nodes would try to send their packets directly to the sink node.

2. RELEVANT KNOWLEDGE

Early approaches proposed for detecting wormhole attacks in wireless ad hoc networks were Packet Leashes [4] and SECTOR [5], which employ the notions of geographical and temporal leashes. The assumption is that each network node knows its exact location, and embeds the location and a timestamp in each packet it sends. If the network is synchronized, then any node that receives these packets can detect a wormhole based on deference in the observed locations and/or calculated times. Such a solution requires a synchronized clock and each node to know its location. The algorithm proposed in this paper does not have these requirements.

Kong, et al. [6] have studied denial-of- service (DoS) attacks (including wormhole attacks) on underwater sensor networks. Because these networks typically use acoustic methods to propagate messages under water, the detection techniques cannot be applied directly to wireless sensor networks.

Hu and Evans [7] have attempted to detect wormholes by equipping network nodes with directional antennas so they can all have the same orientation. Lazos and Poovendran [8] have applied a similar idea in their secure localization scheme called SeRLoc. SeRLoc employs about 400 anchor nodes (called \beacon nodes") in a 5,000-node network. Each anchor node has a directional antenna and knows its physical location. Other nodes in the network use the anchor nodes to locate themselves. Since a wormhole produces shortcuts in a network, the directional antennas deployed in the anchor nodes help detect the attack; nodes can then defend against the attack by discarding incorrect localization messages. However, SeRLoc is unable to detect wormhole attacks when anchor nodes are compromised, especially nodes located near the end of a wormhole.

Multi-path multi-base station data forwarding technique is proposed in [9], in which a sensor node maintains number of different secrets (keys) in a multiple tree. Sensor node can forward its sensed data to multiple routes by using these secrets. There are multiple base stations in the network that have control over specific number of nodes and also, there are common means of communication

among base stations. Each base station has all the secrets that are shared by all the sensor nodes, covered by it, according to the key assignment protocol. Given the shared secret and the generated new key between two sensor nodes, the process of route setup requires much processing hence is inefficient.

In [10] author suggests that hello flood attack can be counteracted by using “identity verification protocol”. This protocol verifies the bi-directionality of a link with encrypted echo-back mechanism, before taking meaningful action based on a message received over that link. This defense mechanism becomes in effective when an attacker has a highly sensitive receiver and a powerful transmitter. If an attacker compromises a node before the feedback message, it can block all its downstream nodes by simply dropping feedback messages. Thus, such an attacker can easily create a wormhole to every node within range. Since the links between these nodes and attacker are bidirectional, the above approach will unlikely be able to locally detect or prevent a “hello flood”.

Considering the scarcity of energy resources of sensor nodes, the authors have proposed in [11] a probabilistic based approach, which forces few randomly selected nodes to report to base station about hello requests. The base station then further analyzes the request authenticity.

In [12] a cryptographic technique is used to prevent the hello flood attack. Any two sensors share the same secret key. Every new encryption key is generated on fly during the communication. This phenomenon ensures that only reachable nodes can decrypt and verify the message and hence prevent the adversary from attacking the network. But the main drawback of this approach is that any attacker can spoof its identity and then generate attacks.

2.1 Typical threats in WSNs

The threats and adequate defense techniques in WSNs can be classified as in Table 1.

Table1. Typical threats in WSNs

Threat	Layer	Defense techniques
Jamming	Physical	Spread-spectrum, lower duty cycle
Tampering		Tamper-proofing, effective key management schemes
Exhausting	Link	Rate limitation
Collision		Error correcting code
Route information. manipulating	Network	Authentication, encryption
Selective forwarding		Redundancy, probing
Sybil attack		Authentication
Sinkhole		Authentication, monitoring, redundancy
Wormhole		Flexible routing, monitoring
Hello flood		Two-way authentication, three-way handshake
Flooding	Transport	Limiting connection numbers, client puzzles
Clone attack	Application	Unique pair-wise keys

3. PACKET TRAFFIC ARRIVAL PROCESS

Because the data traffic dynamics in different WSN scenarios are quite different, the data traffic modeling and analysis in WSNs will be quite application dependent. In [13] it is suggested that WSN applications can be categorized as event-driven or periodic data generation. For periodic data generation scenarios, constant bit rate (CBR) can be used to model the data traffic arrival process when the bit rate is constant [14]. When the bit rate is variable, a Poisson process can be used to model the data traffic arrival process as long as the data traffic is not bursty [15]. For event-driven scenarios such as target detection and target tracking, bursty traffic can arise from any corner of the sensing area if an event is detected by the local sensors. A Poisson process has also been used to model the traffic arrival process in an event-driven WSN [16]. However, there is no solid ground to support the use of a Poisson process in this case. Actually, the widely used Poisson processes are quite limited in their burstiness [17]. Instead of using Poisson processes, the author of this article proposes to use an ON/OFF model (see Figure 1) to capture the burst phenomenon in the source data traffic of an event-driven WSN [18]. Further, the distributions of ON/OFF periods are found to follow the generalized Pareto distribution in his considered WSN scenario. Ref. [19] studies a different WSN scenario - a mobile sensor network (MSN). In an MSN, the node mobility introduces new dynamics to network traffic.

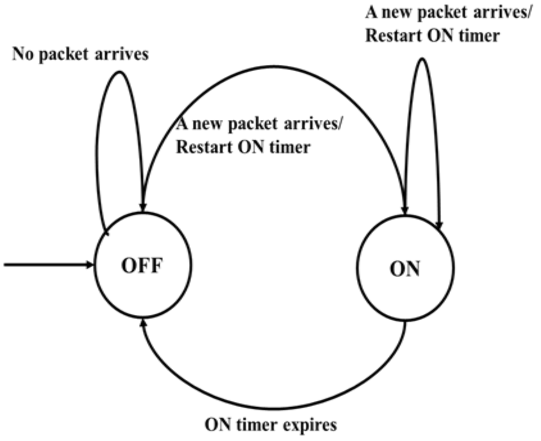

Fig. 1: ON/OFF state transition diagram

In this research have been used constant bit rate (CBR) to modeling the data traffic arrival process when the bit rate is constant (arriving packets to the base station is constant).

4. RULE-BASED INTRUSION DETECTION SCHEMES IN WSN

Also called specification based intrusion detection schemes. In these schemes, the detection rules are first designed by domain expert before the starting the detection process. Most of the techniques in these schemes follow three main phases: data acquisition phase, rule application phase and intrusion detection phase (Silva *et al*., 2005). In the following subsections, the key important schemes in this category are explored.

4.1 Decentralized IDS in WSN

Silva *et al*. (2005) propose the first and the most cited rule-based intrusion detection scheme for WSN to detect many different kinds of attacks in different layers. In this scheme, there are three main phases involved: data acquisition phase in which the monitor nodes are responsible of promiscuous listening of the messages and filtering the important information for the analysis; the rule application phase, in which the pre-defined rules are applied to the stored data from the previous phase, if the message analysis failed any of the rules test, a failure is raised and the counter increased by one; the intrusion detection phase, a comparison is taken place between the number of raised failures produced from the rule application phase with a predefined number of occasional failures that may happen in the network. If the total number of the raised failures is higher, intrusion alarm is produced. According to Xie*et al*. (2011), this scheme brings a good framework to the class of rule-based intrusion detection. But, there is an important drawback of this scheme, which is the ambiguity in determining the number of monitoring nodes dedicated to the detection process, the way of choosing them and how to make sure that the way of selection will cover the entire network. In addition, this scheme is restricted to some types of attacks and the question which may rise up is what if new types of attacks emerge? All these drawbacks should be considered when designing any kind of intrusion detection scheme.

4.2 Malicious Node Detection in WSN

Pires*et al*. (2004) present a solution to identify the possible malicious node based on the received signal strength measured in each node. They showed how to detect two kinds of attacks called HELLO flood attack and the wormhole attack in WSN by building a rule that compare the energy of the received signal and the energy of the same observed signal around the network. Although, this solution was one of the first solutions in the domain, it still restricted to those two types of attacks. In addition, sometimes there are other reasons rather than attacks that may cause a change in the signal strength which make this solution impractical.

4.3 An intrusion Detection System For WSN

A novel intrusion detection scheme that takes the benefits of neighboring node information to detect the node impersonation and resource depletion attacks has been proposed by Onat and Miri (2005). In this scheme each node can make a statistical profile of its neighbor’s behavior based on two features which are the received power rate and the arrival packet rate.

This scheme cannot to be generalized for a typical wireless sensor network application in which many types of attacks evolve continuously. In addition and similar to the scheme proposed in (Pires*et al*., 2004), the building of the rules based on the received power rate is impractical since there are other factors that may affect this feature.

4.4 Towards Intrusion Detection in WSN

Krontiris*et al*. (2007) introduce a lightweight scheme for detecting selective forwarding and blackhole attacks in WSN. The key idea of their scheme is to make nodes monitor their neighborhood and then communicate between each other to decide if there is an intrusion taken place. The scheme is further evaluated experimentally on a real WSN deployment.

This scheme benefits from the neighbors monitoring so that there is a kind of distribution that will minimize the computation load on a detection agent node. However, there will be an increase in the communication messages between nodes during the collaboration for voting that will increase the communication overhead and as a result will deplete the power of nodes quickly. It is clear that, this scheme lacks the generality that other schemes in the same category.

4.5 Intrusion Detection Scheme of Sinkhole Attack in WSN

More specific intrusion detection scheme to detect sinkhole attack was proposed by Krontiris*et al*. (2008). This scheme is composed of four modules: Local Packet Monitoring Module, Local Detection Engine Module, Cooperative Detection Engine and Local Response Model. The proposed scheme has been implemented in the TinyOS environment with MinRoute protocol. A suitable detection rules have been prepared to suite with the sinkhole attack.

Generally, this scheme satisfies the distribution feature of IDS which is highly required on a large scale and autonomous environment like WSN. The problem here still with the communication overhead between the nodes to exchange useful information that helps in detecting the attack.

4.6 Neighbor-Based Intrusion Detection for WSN

Stetsko*et al*. (2010) present an intrusion detection architecture based on collaboration between neighbors. They evaluated their scheme for detecting three types of attacks: Hello flood, selective forwarding and jamming attacks. Their scheme was implemented for Collaboration Tree Protocol (CTP) on the TinyOS environment. Although, the collaboration among nodes makes this scheme strong, the communication overhead is a problem. In addition, the extracted features that are used to construct the rules like packet sending rate and packet dropping rate caused a high false alarm for detecting attacks. Another drawback of this study is that it did not consider the power consumption rate related to the performance which is a very critical issue in WSNs.

4.7 Fuzzy Logic Intrusion Detection Scheme for Directed Diffusion Based Sensor Networks

Chi and Cho (2006) propose an intrusion detection scheme based on fuzzy logic. Some features of the traffic were extracted to build the fuzzy rules which are: node energy level, message transmission rate, neighbor nodes list and error rate in the transmission. The scheme was constructed to prevent and detect from the denial of service (DoS) attack which always drains the resources of the system.

The base station or some monitoring nodes will be responsible for collecting the information messages from the neighborhood and the detection value will be calculated by the fuzzy controller based on the four features mentioned above It is not clear how to choose the monitor nodes and how many nodes will be enough to protect the network. In addition, the need for an expert or sufficient experience to prepare the rule causes inadaptability of the scheme to detect new emerging attacks. Another drawback is that the chosen monitor node can be a point of failure if it is being compromised itself.

4.8 Fuzzy Logic Intrusion Detection Scheme against Sinkhole Attacks in Directed Diffusion Based Sensor Networks

Another fuzzy logic based intrusion detection approach has been proposed by Moon and Cho (2009) to detect sinkhole attacks in directed diffusion based sensor networks. Two features related to the directed diffusion protocols are used which are the reinforcement ratio and the radius. The reinforcement ratio is the proportion of the reinforcement messages transmitted in an area to the number of sensing events from the nodes. The radius is defined as the number of hop counts between any two nodes in the area. In the case of the sinkhole attack, there will be more reinforcement message traffic in area than the normal number and the number of hop count will be smaller. The fuzzy logic controller will use these two features as an input to generate its output which is the detection value. If the result detection value is greater than a predefined security threshold, the controller will raise an alarm that a sinkhole attack has taken place in the area. Prior to the calculation of the detection value, the fuzzy rules should be set by an expert according to the symptoms of the sinkhole attacks.

Using fuzzy logic gives the flexibility of detection sinkhole attacks since the input values are not always sharp values. However, the main problem of any fuzzy based scheme is the need for manual setting of rules.

4.9 Intrusion Detection Based on Traffic Analysis and Fuzzy Inference System in WSN

Ponomarchuk and Seo (2010) introduced an intrusion detection scheme for WSN by utilizing two main traffic features: the packet reception rate and the packet inter-arrival time in a time window and then apply the fuzzy inference to decide whether an attack has taken place or not. However, this scheme is based on fuzzy logic, so it needs the rules to be prepared prior the detection process. The dependence on the prior knowledge which is the rules makes such schemes impractical for a continuous streaming environment like WSN. In addition, the authors did not specify certain attacks to be detected by this scheme.

Advantages of Rule-based intrusion detection schemes for WSN:

- Fast detection: because there is no training involved in these schemes. This feature fulfills the need for online detection when there is a continuous streaming of data in some WSN applications
- The computational complexity is not discussed here: since the schemes use only simple rules for detecting attacks
- Higher detection accuracy: since it depends on comparison with some predefined rules.

5. PROTECTION AlGORITHMS

The system is a cluster type of intrusion detection for wireless sensor networks, its structure after clustering is shown in Figure 2:

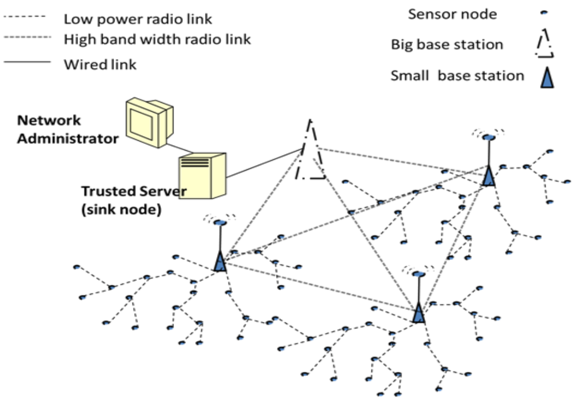

Fig 2. Clustering of wireless sensor networks diagram

In this system, at first, we make the following assumptions:

• In the detection area, each node has the same resources and energy, between nodes is equivalent.

• The node is static in network, and the detection area is divided into clusters by the clustering algorithm, and clustering algorithm can automatically run on the basis of the conditions set by the algorithm.

• The common node of each cluster can directly communicate with the cluster head node or communicate through multi-hop.

• The base station is a safe and unlimited resources, and can communicate with each elected cluster head node, it can form a new cluster with all the cluster head node based the base station on cluster head.

5.1Detection Wormhole attack:

When the network begins work in natural state, number of arrived packets from cluster heads to base station during interval of time is known. We relied on that information to build algorithm to detect wormhole attack.

Algorithm contains these steps:

1- Algorithm is built within the autonomic mechanism.
2- In the natural state of the network, the algorithm saves the number of arrived packets from each cluster head to base station during interval from time (t). Where we get the following table5:

Table5 packet arrived number

Cluster heads IDs	Packets number
ID1	N1 packets
ID2	N2 packets
ID3	N3 packets
.	.
.	.
IDr	Nr packets

3- Calculating the packets number that arriving from cluster heads periodically during the interval of time (t). As shown in figure3.

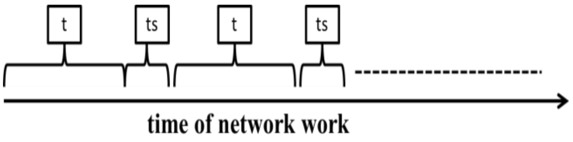

Fig3. Periodic manner of calculating

4.For instance, the number of packets that arrived from cluster head ID3 is n1.
5.Comparing n1 with N3:
6.If n1≈ N3 that means there is no attack on the network.
7.If n1 slightly larger or slightly smaller than N3that means there is no attack on the network.
8.If n1 much smaller than N3, in this case we have two properties:

- There is attack on the network.
- There is physical sabotage on network nodes in that region.

To detect type of that, the base station sends message to all nodes in that region, message commands all the nodes in that region by choosing different path for each sending.

Algorithm after interval time begins to calculate the number of packets that arriving from that region during interval time (t). For instance the number was n3.

If n3 ≈ N3 or n3 slightly larger or slightly smaller than N3that means there was wormhole attack on the network. The algorithm alerts all network components.

If n3 ≈ n1that means there is physical sabotage on network nodes in that region. The algorithm tells the network administrator to repair that region.

5.2 Detection hello flood attack:

When you deploy the network and starting to work, the nodes do these steps:

1- Get neighbors.
2- Count the number of its neighbors.

3- Send its neighbors number and their ID to the main station.
4- Each node owns puzzle used to get to know his neighbors only when you receive order from autonomic mechanism.
5- The autonomic mechanism stores table, this table has the following structure:

Node ID	Neighbors number

In order to detect the attack, autonomic mechanism does the following steps:

1- During specific time periods for each node, each node sends its neighbors number to the autonomic mechanism.
2- The autonomic mechanism tests this value with the stored value.
3- Based on the test result, discovers the attack from autonomic mechanism.
4- The autonomic mechanism sends order to that node in order to use the puzzle to make sure from the neighbors, and detection the hostile node.
5- Node when using the puzzle it detected the hostel node
6- The node alerts all its neighbors.
7- Stop exchanging data with that node.
8- Return to the normal work.

6. PACKE TRAFFIC IN WSN SERVES AS THE DATA SOURCE OF ANOMALY DETECTION

Packet traffic has been the most used data source in the anomaly detection for WSNs. The authors propose that an anomaly in WSNs could violate one of the following rules applied to packet traffic:

1) Interval rule: A failure is raised if the time which passes between the reception of two consecutive messages is larger or smaller than the allowed limits.

2) Retransmission rule: The monitor listens to a message, pertaining to one of its neighbors as its next hop, and expects that this node will forward the received message, which does not happen.

3) Integrity rule: The message payload must be the same along the path from its origin to a destination, considering that in the retransmission process there is no data aggregation by other sensor nodes.

4) Delay rule: The retransmission of a message by a monitor's neighbor must occur before a defined timeout.

5) Repetition rule: The same message can be retransmitted by the same neighbor only a limited number of times.

6) Radio transmission range: All messages listened to by the monitor must have originated (previous hop) from one of its neighbors.

7) Jamming rule: The number of collisions associated with a message sent by the monitor must be lower than the expected number in the network.

By regularly monitoring the violations of the listed rules, network anomalies will be detected.

7. EVALUATING AUTONOMC SYSTEM (ANOMALY DETECTION STRATIGY) FOR WSN

The two commonly used measurements for evaluating the performance of an anomaly detection strategy are the false positive rate (FP) and the false negative rate (FN). FP is defined as the proportion of normal events that are erroneously classified as abnormal. FN is defined as the proportion of abnormal events that are erroneously classified as normal. Obviously, a good anomaly detection strategy should have both a low FP and a low FN. However, a tradeoff is usually to be made between FP and FN, given that these two measurements are usually influenced in opposing ways, by adjusting the threshold parameters used in many anomaly detection strategies. In addition to FP and FN, the overhead introduced by an anomaly detection strategy is also a concern. Considering the extreme resource-constrained specialties of WSNs, a good anomaly detection strategy should introduce as little overhead as possible. Although WSNs are designed for low rate communication, a broad range of real-time applications, such as health care, highway traffic coordination and even multimedia transmission have also been proposed. When an anomaly detection strategy is designed for real-time applications, it should also fulfill the real-time requirement such that it will not cause performance degradation to the applications.

FP is measured as the number of normal records that are classified anomalous. False positive rate (FPR) is the percentage of normal records that are classified anomalous to the total number of normal records as shown in Equation 2 [20].

$$FP = \sum_{t=1}^{t=T} FP(t) \qquad \textbf{Equation 1}$$

$$FPR = \frac{FP}{Total\_normal\_records} \qquad \textbf{Equation 2}$$

The number of normal records in the testing dataset is 3267 and the number of false positive detection is 73 leading to false positive rate of 2.234 %.

FP factor in equation 1 returns the sum of all false alerts within a period of time T. FPR in equation 2 returns the number of false alerts by the total number of collected frames during the same period of time T. FPR measures the percentage of faulty alerts per the total number of received frames. Systems that generate high false positive rates are not practical and less trusted by network administrators.

8. DETECTION RATE

Detection measures the ability of a certain protection systems to detect wireless attacks. This ability is the degree of confidence that an evaluated protection system can indeed detect a certain type of attack. It is quantified as the probability that a certain protection system can detect a certain wireless sensor attacks.

The detection rate (DR) is computed as the percentage of times a certain attack type is detected when attacks from the same type are launched n times as given in Equation 3:

$$DR_j = \sum_{i=1}^{n} \frac{N_{i,j}}{n}, N = \{0,1\} \qquad \textbf{Equation 3}$$

Where ***n*** is the total number of variations for attack type ***j; N(i,j)*** is 1 if the attack is detected and 0 if the attack is not detected. The total detection rate measures the wideness of detection for a certain protection system.

9. RECEIVER OPERATION CHARACTERISTIC

The ROC figure is used by different protection system evaluation methodologies [21], [22], [23] to test and evaluate the accuracy of protection systems. We extend this approach to evaluate the protection system operation by considering both false alarms and detection rates. ROC shows the detection rate variations against higher or lower false-positive rate. While detection rate quantifies the ability of protection system to detect certain attacks, a high false positive rate can degrade the trust level because detection alerts might not be taken seriously by system administrators.

Consequently, ROC represents the degree of confidence in attack detection alerts produced by the protection system. To experiment with different variations of wireless attacks, the evaluated protection systems are tested several times against each type of attack. A direct comparison of the accuracy between protection system and AirDefense is shown in Figure 4, where protection system provides a higher detection rate and a lower false positive rate.

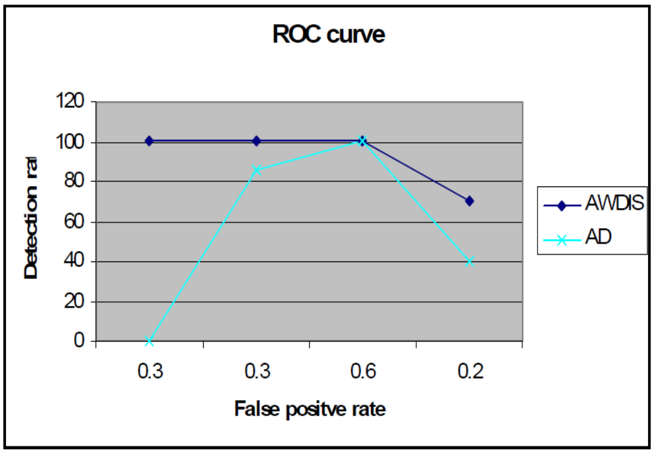

Fig 4.ROC Curve showing direct comparison between WSPS and AirDefense for 4 different types of attacks.

10. EXPERIME_TAL RESULTS

10.1 Simulation parameters:

Ns-2 simulator will be used to evaluation our work. Ns-2 is an object-oriented (OO) simulator, written in C++, with an OTcl interpreter as a front-end [24]. Simulation kernel, models, protocols and other components are implemented in C++, but are also accessible from OTcl. OTcl scripts are used for simulator configuration, setting up network topology, specifying scenarios, recording simulation results etc. Typical ns-2 OTcl script for wireless simulation begins with configuration command, which is used to specify PHY, MAC and routing protocol, radio propagation and antenna model, topology etc. The next step is creation of mobile nodes. Node movement and network traffic patterns are usually defined in separate files. Tools for generating these files are provided. The table 2 shows the simulation parameters:

Table 2. Simulation parameters

channel type	Wireless Channel
radio-propagation model	Propagation/Two Ray Ground
network interface type	Phy/Wireless Phy/802_15_4
MAC type	Mac/802_15_4
interface queue type	Queue/DropTail/PriQueue
link layer type	LL
antenna model	Antenna/Omni Antenna
max packet in ifq	100
number of sensor nodes	80
protocol type	AODV
X dimension of topography	500 m
Y dimension of topography	500 m
simulation period	500 second
Energy Model	Energy Model
value	Initial energy 100
number of CH (cluster head) nodes	8
number of base station node	1

10.2 RESULTS

The detection rates of wormhole and hello flood attacks are shown in Table 3.

Table 3. Detection Rate (DR) for wormhole and hello flood attacks

Type	Size	Number of Detection	DR
Wormhole	400	387	96.60%
Hello Flood.	400	377	94.15%

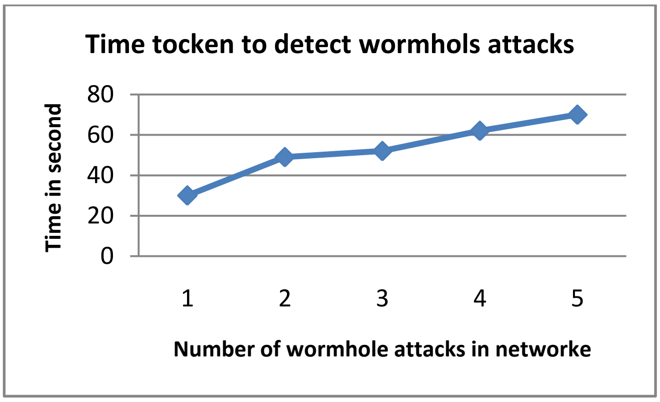

Fig5. Time token to detect wormhole attack

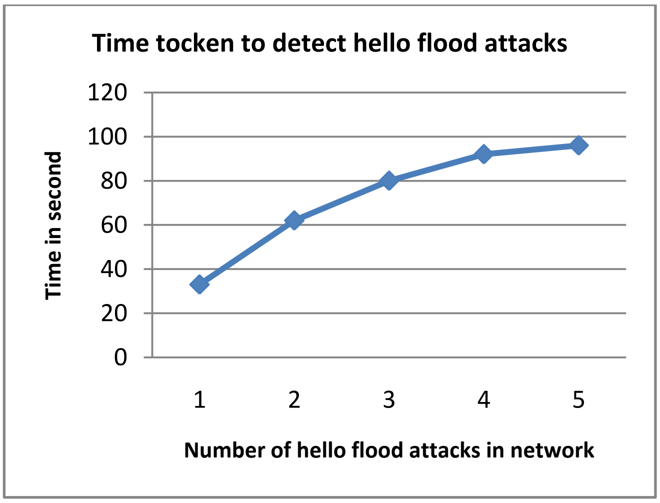

Fig6. Time token to detect wormhole attack

Figures 5 and 6 show the time necessary to detect attacks when using our algorithms.

11. CONCLUSION

This paper analyzes the characteristics of wireless sensors, and in order to detect the threat of attack, for there are some external attack and internal attack in wireless sensor networks, we proposed tow algorithms for wireless sensor networks based on rule learning and packet flow rat.

Our algorithms no needing additional requirements, because they are built in base station.

Depending on the simulation results, our algorithms are Very effective.

The aim of our future research is to choose appropriate characteristics to reduce false rate and increase the accuracy when detecting attacks.

12. REFERENCES

[1] Zhenwei Yu, Jeffrey J.P. Tsai,A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing,2008.

[2] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: defense against wormhole attacks in wireless ad hoc networks. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003.

[4] Y. Hu, A. Perrig and D. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1976-1986, 2003.

[5] S. Capkun, L. Buttyan and J. Hubaux, SECTOR: Secure tracking of node encounters in multi-hop wireless networks, Proceedings of the First ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21-32, 2003.

[6] J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia and B. Bhargava, Lowcost attacks against packet delivery, localization and time synchronization services in underwater sensor networks, Proceedings of the Fourth ACM Workshop on Wireless Security, pp. 87-96, 2005.

[7] L. Hu and D. Evans, Using directional antennas to prevent wormhole attacks, Proceedings of the Eleventh Network and Distributed System Security Symposium, pp. 131-141, 2004.

[8] L. Lazos and R. Poovendran, SeRLoc: Robust localization for wireless sensor networks, ACM Transactions on Sensor Networks, vol. 1(1), pp. 73-100, 2005.

[9] A Hamid, S Hong, (2006) Defense against Lap-top Class Attacker in Wireless Sensor Network, ICACT

[10] Venkata C. Giruka, MukeshSinghal, James Royalty, Srilekha Varanasi, (2006), Security in wireless networks, Wiley Inter Science.

[11] Dr. Moh. Osama K., (2007),Hello flood counter measure for wireless sensor network, International Journal of Computer Science and Security, volume (2) issue (3).

[12] Chris Karlof, David Wagner,(2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE.

[13] Demirkol, I., Alagoz, F., Delic, H., and Ersoy, C. (2006). Wireless sensor networks for intrusion detection: Packet traffic modeling. IEEE Communications Letters, 10(1):22--24.],

[14] Cui, S., Madan, R., Goldsmith, A. J., and Lall, S. (2005). Joint routing, mac, and link layer optimization in sensor networks with energy constraints. In Proc. of IEEE International Conference on Communications (ICC'05), pages 725--729.

[15] Ma, Y. and Aylor, J. H. (2004). System lifetime optimization for heterogeneous sensor networks with a hub-spoke topology. IEEE Transactions on Mobile Computing, 3(3):286--294.

[16] Tang, S. (2006). An analytical traffic flow model for cluster-based wireless sensor networks.In Proc. of 1st International Symposium on Wireless Pervasive Computing.

[17] Paxson, V. and Floyd, S. (1995). Wide-area traffic: The failure of poisson modeling. IEEE/ACM Transactions on Networking, 3:226--244.

[18] Wang, Q. and Zhang, T. (2008). Source traffic modeling in wireless sensor networks for target tracking. In Proc. of the 5th ACM International Symposium on Performance Evaluation of Wireless Ad-Hoc, Sensor, and Ubiquitous Networks (PE-WASUN'08), pages 96--100.

[19] Wang, P. and Akyildiz, I. F. (2009). Spatial correlation and mobility aware traffic modeling for wireless sensor networks.In Proc. of IEEE Global Communications Conference (Globecom'09).

[20] W. Lee, S. J. Stolfo K. Mok, “A data mining framework for building intrusion detection models”, In Proc. IEEE Symposium on Security and Privacy, 1999.

[21] SJ Stolfo, W Lee, PK Chan, W Fan, E Eskin “Data mining-based intrusion detectors: an overview of the columbia IDS project” ACM SIGMOD Record, 2001 -portal.acm.org.

[22] Lippmann et al. “Evaluating intrusion detection systems: The 1998 DARPA offline intrusion detection evaluation”, In Proceedings of the on DARPA Information Survivability Conference and Exposition (DISCEX’00).

[23] J. McHugh. Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory.

[24] K. Fall and K. Varadhan, “The ns manual”, User’s manual, UC Berkeley, LBL, USC/ISI, and Xerox PARC, January 2009.