Hosamsoleman, Ali Payandeh, Nasser Mozayyani, SaeedSedighianKashi/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp.261-268

Detection Collision Attacks In Wireless Sensor Network Usingrule-Based Packet Flow Rate

Hosamsoleman[1], Ali Payandeh[2], Nasser Mozayyani[3], SaeedSedighianKashi[4]

[1,2](Department of Computer Engineering Maleke-Ashtar University Islamic Republic of Iran)

[3](School of Electrical & Computer Engineering.Elm-o-SanatUniversity Islamic Republic of Iran)

4(School of Electrical & Computer Engineering.K.N toosi University of TechnologyIslamic Republic of Iran)

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. In this paper, we consider the collision attack that can be easily launched by a compromised (or hostile) node: a compromised node does not follow the medium access control protocol and cause collisions with neighbor transmissions by sending a short noise packet. This attack does not consume much energy of the attacker but can cause a lot of disruptions to the network operation. Due to the wireless broadcast nature, it is not trivial to identify the attacker. This paper describes detection algorithms for wireless sensor networks, which detects collision attack 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, collision attack.

I. 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, collision 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 collision Attack [2].

In the collision attack [2], the adversary sends his own signal when he hears that a legitimate node will transmit a message in order to make interferences. In theory, causing collisions in only one byte is enough to create a CRC error and to cripple the message. The advantages of a collision attack are the short power energy consumed and the difficulty to detect it (the only evidence of collisions attacks is incorrect message). In fact, such an attack can target specially the ACK control message causing an exponential back-off in some MAC protocol. According to attack attributes, first the intention of the collision attack is to exhaust the battery by using the channel of communication indefinitely. Then in the movement class, the attacker does not really need particular technical capabilities and it can be launched by anyone in the network, the vulnerability is the data integrity requirement and the layer used is the link layer. The target is general logical and can be at the same time against internal service like power management and against provided services, for example the communication service. Finally the result can be partial degradation if the attack is launched in certain region in the network or total degradation if the attack is applied in multiple precise locations in the network.

II. RELEVANT KNOWLEDGE

Marti et al. [3] discussed two techniques that detect compromised nodes that agree to forward packets but fail to do so. The authors use watchdogs that identify misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. When a node forwards a packet, the nodes watchdog verifies that the next node in the path also forwards the

packet. The watchdog does this by listening promiscuously to the next nodes broadcast transmissions. If the next node does not broadcast the packet, it is misbehaving and the watchdog detects it. Every time a node fails to forward a packet, the watchdog increments the failure-tally. If the tally exceeds a certain threshold, it is determined that the node is misbehaving; this node is then avoided with the help of the pathrater. The pathrater combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. The overhead of passive continuous passive listening is formidable for WSNs.

Buchegger et al. [4] proposed a mechanism that detects misbehaving nodes by means of observations or reports about several types of attacks. This allows nodes to find routes around misbehaving nodes and to isolate them from the network. Nodes have a monitor for observations, reputation records for first-hand observations and trusted second-hand reports, trust records to control trust given to received warnings, and a path manager to adapt their behavior according to reputation of other nodes. This approach involves continuous monitoring similar to Marti.s approach and collecting information about intrusion detections at other places in the network. The overhead is prohibitive for WSNs.

Michiardi et al. [5] proposed a collaborative reputation mechanism that has a watchdog component. However, it is complemented by a reputation mechanism that differentiates between subjective reputation (observations), indirect reputation (positive reports by others), and functional reputation (task specific behavior). They are weighted for a combined reputation value used to make decisions about cooperation with or gradual isolation of a node. This approach involves continuous monitoring and collecting information about intrusion detections at other places in the network for specific functions. The overhead is too high for WSNs.

Huang et al. [6] proposed a mechanism that needs separate monitoring nodes, specifically one monitor per cluster (nodes that are in one-hop range from a cluster). The approach requires monitors to be active. If there is one monitor per cluster, the monitor does most of the work. In WSNs, there is a risk that monitor nodes run out of energy before the network does or before the network gets partitioned. This contradicts one of the main goals of prolonging WSN lifetime and keeping WSN connected as much as possible (since battery replacement is a very costly or unavailable alternative).

All the above approaches monitor individual nodes all the time. Continuous monitoring of each and every node is not feasible for resource-constrained WSNs especially when extending lifetime is the main goal in the design of WSNs. Our proposed solution, protect WSN from collision 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

III. 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.

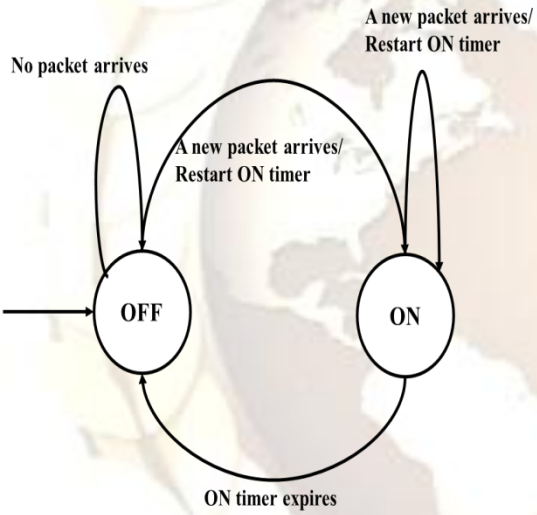

Fig. 1: ON/OFF state transition diagram

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).

IV. 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.

V. PROTECTION AlGORITHMS

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

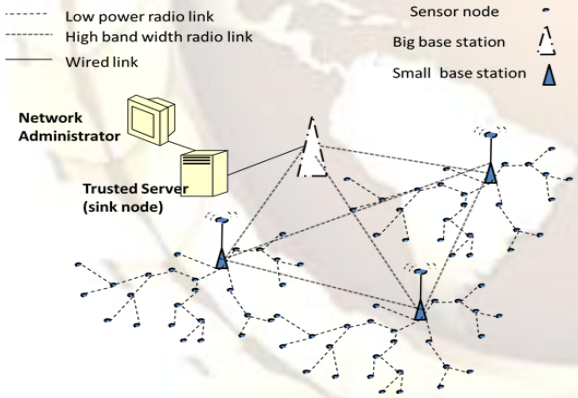

Fig 2. Clustering of wireless sensor networks diagram

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- Storing packet delivery waiting time (M) and packet collision ratio (N) for period (PDR) of time (ts) during the normal work of the network without the presence of an attack for each cluster head, and storing that information in the table that shown in table

Cluster heads IDs	Packets delivery waiting time	Packet collision ratio
ID1	M1	N1
ID2	M2	N2
ID3	M3	N3
.	.	.
.	.	.
IDr	Mr	Nr

2- For each period of time (t2) the autonomic mechanism tests the packet delivery waiting time and packet collision ratio for each cluster head. For example, the value of packet delivery waiting time and packet collision ratio of cluster head x is M and N respectively in normal work of network, and the value of packet delivery waiting time and packet collision ratio during testing the PDR from autonomic mechanism is M1 and N2 respectively.

3- Comparing M1 and M.

4- Comparing N1 and N.

5- Depending on that comparing the autonomic mechanism determines if there attack or no.

6- If there attack, the autonomic mechanism alerts the cluster head and determines the location of attack based on information in the packet format (packet information).

VI. 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.

VII. 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].

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

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

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.

VIII. 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:

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

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.

IX. RECEIVER OPERATION CHARACTERISTIC

The ROC figure is used by different protection system evaluation methodologies [21, 22, and 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.

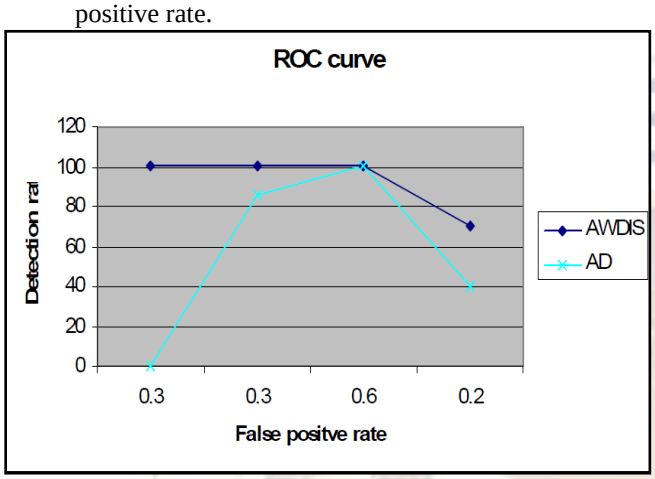

Fig 4.ROC Curve showing direct comparison between WSPS and AirDefense for 4 different types of attacks.

X. 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 collision attacks are shown in Table 3.

Table 3. Detection Rate (DR) for collision attacks

Type	Size	Number of Detection	DR
Collision attack	350	320	96.60%

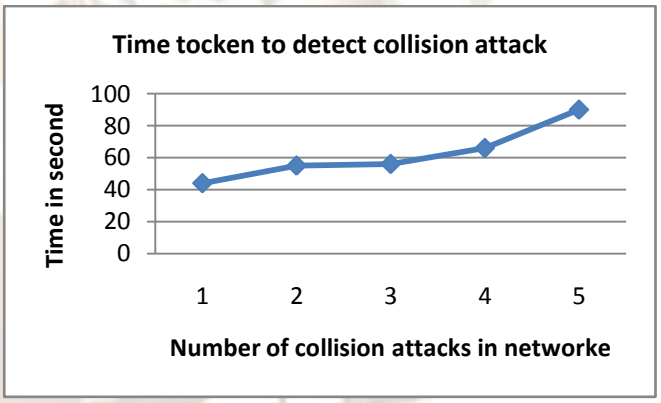

Fig5. Time token to detect collision attack

Figures 5 shows the time necessary to detect attacks when using our algorithms.

XI. 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 algorithm 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.

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] W. Znaidi, M. Minier and J. P. Babau; An Ontology for Attacks in Wireless Sensor Networks; INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA); Oct 2008.

[3] Marti, S., Giuli, T. J., Lai, K., and Baker, M., .Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,. Proc. 6th Annual Intl. Conf. on Mobile Computing and Networking (MobiCom.00), Boston, Massachusetts, August 2000, pp. 255-265.

[4] Buchegger, S. and Le Boudec, J., .Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes -Fairness in Dynamic Ad-hoc Networks., Proc. 13th IEEE/ACM Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc), Lausanne, Switzerland, June 2002.

[5] Michiardi, P. and Molva, R., .CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks., Proc. IFIP 6th Joint Working Conference on Communications and Multimedia Security (CMS.02), Portoro., Slovenia, September 2002, pp. 107-122.

[6] Chen, Z. and Khokhar, A., "Self Organization and Energy Efficient TDMA MAC Protocol by Wake Up For Wireless Sensor Networks", Proc. First Annual IEEE Intl Conf. on Sensor and Ad Hoc Communications and Networks (SECON 2004), Santa Clara, CA, October 2004.

[7] 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.],

[8] 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.

[9] 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.

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

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

[12] 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.

[13] 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).

[14] 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.

[15] 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.

[16] 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).

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

[18] K. Fall and K. Varadhan, "The ns manual", User's manual, UC Berkeley, LBL, USC/ISI, and Xerox PARC, January 2009.