International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 6 (2018) pp. 4214-4218

Implementation of Advanced IDS in Contiki for Highly Secured Wireless Sensor Network

R.Darwin

Assistant Professor, Department of Electronics and Communication Engineering, Kumaraguru College of Technology, Coimbatore, India.

Abstract

The security threats for 6LoWPAN will be from within the 6LoWPAN network or from the IP network. The security techniques which are used for wireless environment in LoPAN devices as the major line of defense will be more susceptible to intruders due to the weak nature of LoPAN devices in wireless environments. Nodes could prompt insider assaults without being distinguished by any cryptography checking. An intrusion detection system (IDS)[1] is principally required as a moment line of resistance to screen the system operations and bring an alert up if there arises an occurrence of any inconsistency. This project examines potential security dangers in 6LoWPAN and audits the present countermeasures specifically the IDS-based answers for countering insider/inner dangers.

Keywords: IDS, RPL, IoT, security, WSN, Contiki, COOJA

INTRODUCTION

The concept of Internet of Things (IoT) is a new wave in the technology market that came into existence for reducing the gap between small devices and the IP world making them smart. 6LoWPAN is a technology developed for low power personal area network based on IP. One of the key issues in 6LoWPAN is implementing IDS. There are many low power operating systems that support IDS such as TinyOS and Contiki. These operating systems are widely used to implement Internet of Things. Routing Protocol for Lossy and Low Power Network (RPL) is based on Directed Acyclic Graph (DAG). Though a DAG resembles a tree like structure, nodes in a DAG can have multiple parents whereas trees permit only one parent. RPL organizes as Destination Oriented DAGs (DODAG) in which the popular destination node or a node with internet access is taken as the root. IDS[1] can be implemented based on this DODAG information. Contiki is an open source operating system that has been designed specifically for IoT. It enables even a tiny, low-power microcontroller to access internet. It supports IPv6 and IPv4 standards. It also supports recent low-power wireless standards like 6LoWPAN, RPL and CoAP. It uses Contiki MAC and sleepy routers which enables the nodes to operate with very low power that facilitates battery operation. COOJA is a Contiki network simulator. As Contiki devices generally make up large networks, developing and debugging becomes very difficult. COOJA provides a simulation environment which makes this task tremendously easy. This project analyses IDS implementation using Tmote sky mote which is supported by COOJA. Tmote Sky is an ultra low power remote module that finds wide utility in sensor systems, checking applications and fast application prototyping. Tmote Sky use industry norms like USB and IEEE 802.15.4 to interoperate consistently with different gadgets.

RELATED WORKS

Bhuse et al. [2] proposed lightweight strategies to identify oddity interruptions in remote sensor systems. He reused the effectively accessible framework data that is created at different layers of a system stack. Farooqi et al. [3] presented a survey of various IDS mechanisms such as distributed mechanism, purely centralized and distributed-centralized mechanism. He explained the use of IDS to prevent denial of service, routing attack and Sybil attack. Gupta et al. [4] proposed ANDES as a framework for detecting and finding the root causes of anomalies in operational wireless sensor networks. He correlates information from two sources: one in the data plane as a result of regular data collection in WSNs and the other in the management plane implemented via a separate routing protocol, making it resilient to routing anomaly in the data plane. Ahmed et al. [5] proposed a new approach of abnormal node detection in wireless sensor network using IDS security routing methodology by dividing the network into number of pairs. The algorithm uses both signatures and knowledge based routing methodology to detect the abnormality of the nodes.

Shaikh et al. [6] proposed a validation algorithm to improve the reliability and reduces the false alarms. Li et al. [7] proposed a disseminated assemble based interruption identification plot that gives a productive lightweight interruption location calculation. He considered the numerous qualities of the sensor hubs to distinguish noxious assailants accurately and lessened the false caution rate. De Sousa Lemos et al. [8] proposed a new collaborative and decentralized approach for intrusion detection system that reduces the false positives. He used special nodes, called monitors that will be responsible for monitoring the behavior of neighbor nodes. Hai et al. [9] has explained the need for IDS in wireless sensor network. Mubarak et al. [10] proposed a method which selects a set of trusted nodes and does the intrusion detection only with this set of nodes. This selection algorithm helps in energy efficiency as the information is routed only through these set of nodes. Le et al. [11] has given the need for IDS in 6LoWPAN. Yan Zhang et al. [12] proposed a decision support system for constructing an alert

classification model, which consists of three phases: alert preprocessing, model constructing and rule refining. Zhou et al. [13] proposed a hybrid intrusion detection model based on the parallel genetic algorithm and the rough set theory. The application of hybrid genetic algorithm in solving the rough set reduction saves computing time. Pereira et al. [14] proposed an IDS method by using non supervised learning. He used clustering to create IDS rules. Qingsong et al. [15] proposed an embedded architecture of SPMOS- based IDS and this improves the efficiency of the system. Paulo M. Mafra et al. [17] proposed a distributed IDS model for mobile ad hoc networks that can identify and punish those network nodes that have malicious behavior. Liu et al. [16] presented a study work for distributed denial of service. He also proposed a Q function based learning detection.

PROPOSED IDS ARCHITECTURE

The network performance can be guaranteed by the following parts:

(i) RPL specification-based IDS to monitor 6LoWPAN optimized topology

(ii) Anomaly-based IDS used in cooperation with specification-based IDS to monitor the node performance

(iii) Statistical-based component to reveal the attacker source

Tracking back a component can be analyzed using statistical techniques. The proposed model will attempt to predict the network nodes that behave maliciously, by analyzing statistical data from the monitoring nodes in the network.

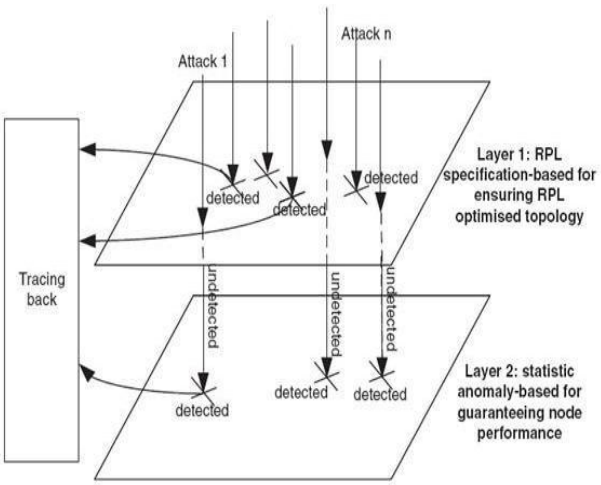

Figure 1. Two Layer Architecture of IDS

Fig. 1 depicts the two layer architecture of IDS. Layer 1 is the RPL specification-based IDS for detecting all the threats that violate RPL's operation rules for ensuring optimized network topology. Layer 2 is the anomaly-based IDS that ensure node performance. When the malicious behavior of a mote is detected, the system will be processed to trace back the attacker node. The network QoS can be assured by eliminating the malicious mote. This system can provide a robust security countermeasure for the 6LowPAN. By adding other protection layers, the system can be expanded. But they should work in cooperation with previous layers. The new protection layer should only aim at the attacks that cannot be detected by previous layers. RPL is the underlying routing protocol for 6LoWPAN. So building a specification based IDS for RPL is one of the most efficient way to detect fast and accurate 6LoWPAN attacks that break its optimized topology set up. Initial work on securing RPL focuses on protecting RPL control messages (DIO, DIS and DAO) and the routing information in IPv6 Hop-by-Hop Option Header and Routing Header. The architecture for intrusion detection in 6LoWPAN is shown in Fig. 2.

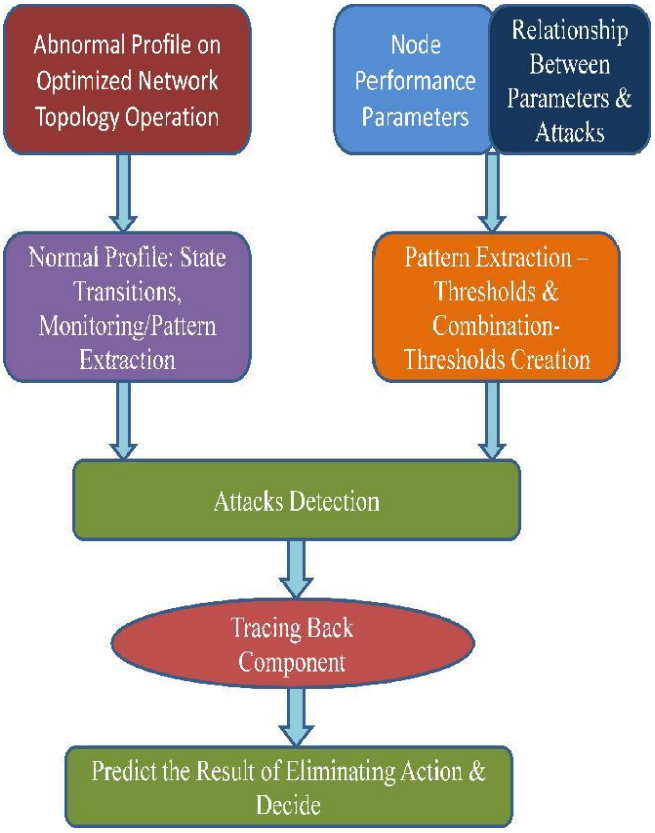

Figure 2. IDS Architecture in 6LoWPAN

The IDS will collect the RPL routing information and check the state of control messages transmissions to detect the routing attacks. Each monitoring mote will observe the communications between the monitored motes to extract the topology information, mostly the parent–child relationship to detect anything invalid in the topology. Besides that, any topology change will be remembered and a threshold is defined so that if a node creates too many changes in its relationships, an alarm will be raised. The anomaly-based IDS will analyze the relationships of those network parameters in the event of attacks as symptoms to diagnose the attacks or to prevent future attacks.

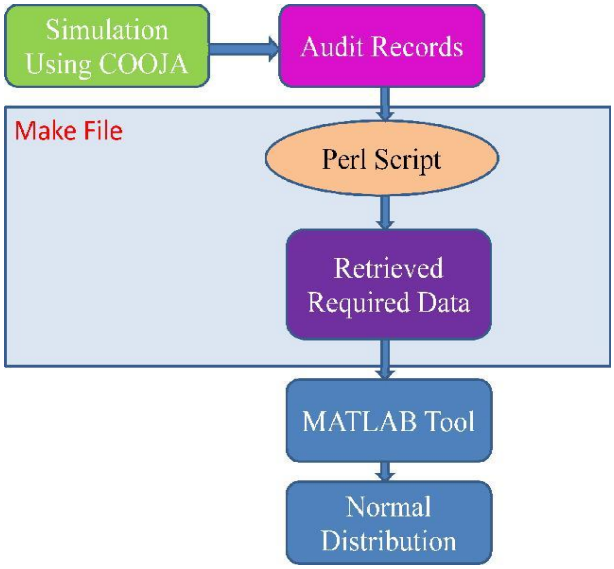

Figure 3. IDS Implementation steps in Contiki

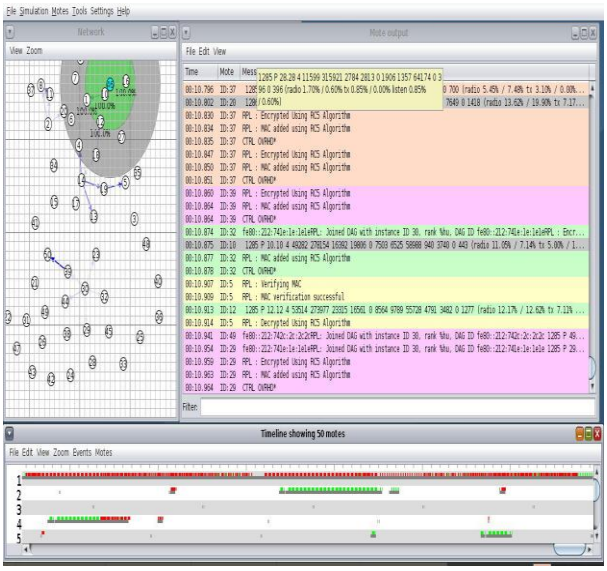

Figure 4. COOJA Setup Screenshot

The steps for implementing IDS in Contiki (Fig. 3) are:

1. Run the WSN network in COOJA simulator and get the log output.
2. From this log output the required audit records are taken out by using PERL script.
3. These audit records are imported in the MATLAB tool and processed.
4. So that, the distribution for the data set can be obtained and the pattern will be defined.
5. If any node varies from this pattern, then an alarm will be generated and thus the anomaly node can be detected.

There are many threats and attacks [12] that are overcome by secure IDS.

RESULTS

A. Simulation Setup:

The operating system used is ubunto linux 14.04 with 4 GB RAM to accommodate the simulation load. The simulation is done using java based COOJA simulator for Contiki based networks. The mote used is Tmote sky. The simulation is done using 20, 50 and 100 motes. The mote output during simulation is stored in a log file. Perl script is a scripting language that is used to process the log files and generates the required output. The screenshot of COOJA is shown in Fig. 4.

B. IDS Analysis:

The analysis and implementation of IDS are done by mimicking the behaviors of an intruder. And also the abnormal behaviors could be detected by comparing the behavior of the suspected mote to the general behavior of the network motes.

C. Analysis of ICMPv6 Messages:

There are three types of control messages. They are,

1. DIO (DODAG Information Object)
2. DIS (DODAG Information Solicitation)
3. DAO (Destination Advertisement Object)

The DIS is used to solicit DIO from neighboring nodes. Through DIO the node learns the required parameters to join the DAG and then it sends a DAO upwards along the route. In order to implement IDS, the analyses of these control messages are vital. The intruder node if any, will try to solicit the information object from the neighboring nodes quite often compared to authentic nodes. The amount of control messages varies according to the configuration in ContikiRPL. Initially we analyze the control messages for the default configurations in Contiki RPL. The analysis mainly comprises of total number of each control messages and the frequency in which each control messages are sent. Based on the results we define the threshold in the monitoring mode, which can be used to verify the abnormal patterns of the monitored motes.

D. DIO Pattern:

The frequency of DIO messages are obtained from the audit record. The distribution for the frequency of DIO messages is shown in the Fig. 5. If DIO messages received fall consistently outside this interval then it is considered as an abnormal behavior.

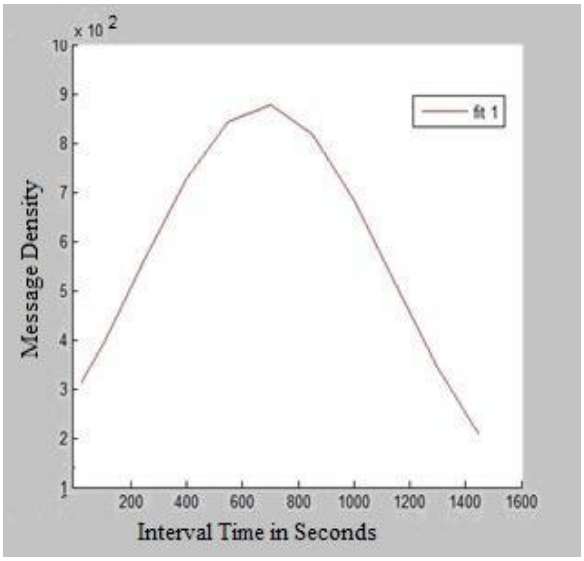

Figure 5. Distribution for DIO Messages

E. DIS Pattern:

Normally the first message a mote sends after startup is a solicitation message (DIS) to get the information object from the neighboring mote (DIO). Since DIO is a broadcast message, the solicitation request from any mote will trigger the receiving mote to broadcast DIO. If a mote receives a broadcasted DIO before sending a solicitation message, the mote will not send the solicitation message. So, the result of the analysis is that when a network is setup, few motes broadcast DIS which triggers DIO that are received by other motes, even before they solicit for information. So, only a few motes sends DIS and other motes do not send DIS. If the mote is an intruder, in order to gain more information from the network, the solicitation message will be continually broadcasted, which is not a normal behavior. The distribution for DIO message and DIS message count is shown in the Fig. 6. From the simulation results, the number of DIO messages received by all the motes is same except the server mote.

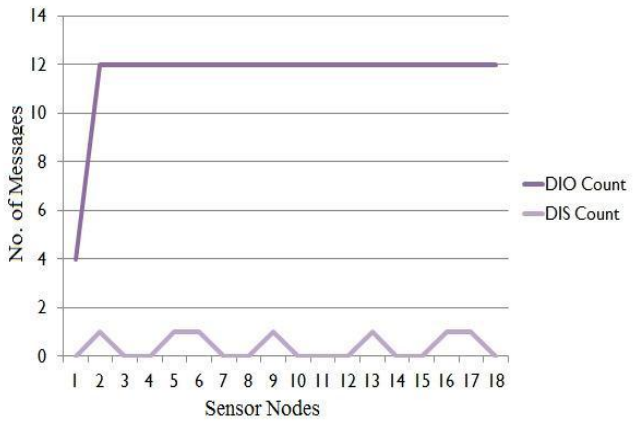

Figure 6. DIO and DIS Message Count

F. Change in Parents and Routes:

Since ContikiRPL is a self organizing network, the best route and parent are calculated and assigned in each mote. An intruder will look to find more information by changing the parents and consequently the routes. Frequent change in parents, routes and deviation from optimum parents and routes is considered as an abnormal behavior.

CONCLUSION

The analyses done are for default ContikiRPL configuration. The network might have different Contiki implementation to improve convergence time to reduce overhead, etc.. So, if the configuration changes, the analysis of the control messages will change accordingly. So, the design is in progress to implement a real time analysis and to monitor to facilitate flexibility in the configuration changes in ContikiRPL. Since we try to implement IDS on 6LoWPAN network which is related to IOT, a web server is launched in the monitoring mote to facilitate the user to see for himself, the behavioral details of monitored motes from his browser.

REFERENCES

[1] Ioannis, Krontiris, Tassos Dimitriou, and Felix C. Freiling, "Towards intrusion detection in wireless sensor networks," *Proc. of the 13th European Wireless Conference*, 2007.

[2] Vijay Bhuse, and Ajay Gupta, "Anomaly intrusion detection in wireless sensor networks," *Journal of High Speed Networks, Vol.* 15.1, pp. 33-51, 2006.

[3] Ashfaq Hussain Farooqi, and Farrukh Aslam Khan, "Intrusion detection systems for wireless sensor networks: A survey," *Communication and networking*. Springer Berlin Heidelberg, pp. 234-241, 2009.

[4] Sumit Gupta, Rong Zheng, and Albert MK Cheng, "ANDES: an anomaly detection system for wireless sensor networks," *Mobile Adhoc and Sensor Systems, MASS 2007 IEEE Internatonal Conference on*. IEEE, 2007.

[5] Khandakar Rashed Ahmed , A.S.M Shihavuddin, Kabir Ahmed, Md. Shirajum Munir, and Md Anwar Asad, "Abnormal node detection in wireless sensor network by pair based approach using IDS secure routing methodology," *International Journal of Computer Science and Network Security,, Vol.* 8-12, pp. 339-342, 2008.

[6] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. D'Auriol, Sungyoung Lee, Young Jae Song, and Heejo Lee, "Trusting anomaly and intrusion claims for cooperative distributed intrusion detection schemes of wireless sensor networks," In Proceedings of the 9th International Conference for Young Computer Scientists, IEEE, pp. 2038-2043, 2008.

[7] Guorui Li, Jingsha He, and Yingfang Fu, "Group-based intrusion detection system in wireless sensor networks," *Computer Communications, Vol.* 31-18, pp, 4324-4332, 2008.

[8] Marcus Vinícius de Sousa Lemos, Líliam Barroso Leal, and Raimir Holanda Filho, "A New Collaborative Approach for Intrusion Detection System on Wireless Sensor Networks," *Novel Algorithms and Techniques in Telecommunications and Networking*. Springer Netherlands, pp. 239-244, 2010.

[9] Tran Hong Hai, Eui-Nam Huh, and Minho Jo, "Lightweight Intrusion Detection for Wireless Sensor Networks," *Intrusion Detection Systems,* Pawel Skrobanek (Ed.), InTech, pp. 559-572, 2011.

[10] T. Mohamed Mubarak, Syed Abdul Sattar, Appa Rao, and M. Sajitha, "A Collaborative, Secure and Energy Efficient Intrusion Detection Method for Homogeneous WSN," *Advances in Computing and Communications*. Springer Berlin Heidelberg, pp. 102-110, 2011.

[11] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Mahdi Aiash, and Yuan Luo, "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach," I*nternational Journal of Communication Systems*, Vol. 25-9, pp. 1189 - 1212, 2012.

[12] Yan Zhang, Shuguang Huang, and Yongyi Wang, "IDS Alert Classification Model Construction Using Decision Support Techniques," *International Conference on Computer Science and Electronics Engineering*, 2012.

[13] Fen Zhou, and Gaizhen Yang, "Network intrusion detection using rough sets based parallel genetic algorithm hybrid model," *International Symposium on Intelligence Information Processing and Trusted Computing*, 2010.

[14] Hermano Pereira, and Edgard Jamhour, "A Clustering-Based Method for Intrusion Detection in Web Servers," *Telecommunications (ICT), 20th International Conference*, 2013.

[15] Shi Qingsong, Chen Du, Nan Zhang, Jijun Ma, and Tianzhou Chen, "SPMOS-based Intrusion Detection Architecture," *Fifth IEEE International Symposium on Embedded Computing,* 2008.

[16] Lei Liu, "A Heuristic Detection Network," *Operator-Assisted (Wireless Mesh) Community Networks*, 2006.

[17] Paulo Manotel Mafra, Joni da Silva Fraga, and Altair Olivo Santin, "A Distributed IDS for Ad Hoc Networks." *26th International Conference on Advanced Information Networking and Applications Workshops*, 2012.