IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. IV (Nov.-Dec. 2016), PP 104-108
www.iosrjournals.org

EXHIPS: Extending the Span of 6LowPAN Networks by Propagating Malicious Node Alert Message

A.Jahir Husain[1], M.A.Maluk Mohamed[2]
[1]Research Scholar, Software System Group, M.A.M.College of Engineering, India
[2]Professor, M.A.M.College of Engineering, India

Abstract:*In this paper, we propose a hybrid, Intrusion Prevention architecture for Internet of Things. This is an extension of our previous architecture Hierarchical Intrusion Prevention System (HIPS). In this both centralized and distributed methods are used to eradicate the Denial of Sleep attack in IoT when it is deployed in a widerrange. We evaluate the performance by simulatingthe network and comparing with other existing systems. Thesimulation results confirm that our systemis performing betterthan other systems in terms of extending the life time of IoT nodes.*

Keywords:*Hybrid Systems, Internet of Things, Intrusion Prevention, Malicious Node Alert*

I. Introduction

In the predictable future, billions of low power wireless devices are expected to be connected to the Internet. These low power wireless networks are enabled with 6LoWPAN protocol which follows the IEEE 802.15.4 standard. This creates the new network paradigm called the Internet of Things (IoT) where Internet Protocol could be applied even to the smallest devices. IoT combines the features of Wireless Sensor Networks for reading the environment and Ad hoc Networks for communication. In IoT, each node is enabled with a 6LoWPAN radio, wireless sensors anda built in battery.A node in IoTis functioning with either a microcontroller based or Linux based embedded platform.An important component of anyIoT network is the Border Router (6LBR) that hooks up the nodes to the Internet. In IoTthe Border Router(6LBR)nodetakes care of transmitting the information sent by the Wireless Sensor Nodes and sends it to the IPv4/ IPv6 server by using the Ethernet IPv4/IPv6 interface. The BR is working as a gateway between two different link-layer technologies, in general 802.15.4 on the WSN side, and the Ethernet or Wi-Fi on the internet side [1]. Each Border Router/Gateway Node is functioning with a Linux based Single Board Computer, 802.15.4 transceiver, an Ethernet interface and a battery.Since Wireless Sensor Network (WSN) is the building block of the Internet of Things (IoT), most of the energy related issues of WSN become common to IoT also. WSNs are well known for their resource-constrained nature in various aspects. The most challenging issue is the limited battery power of the sensors due to the built in batteries.The next challenging issue is thelowcomputational capability, which is due to the built in tiny processor and the limited memory capacity. These issues make the WSN prone to energy-drain attacks, particularly the denial-of-sleep attack[2].

Existing solutions for tackling these attacks in WSN rarely consider the future expansion of the IoT as predicted its expansion in coming years[3]. Hence there should be a solution which is not just energyefficient but, independent, self-sufficient in nature in order to survive the variety of attacks. In this paper we propose an architecture which is an extension of our previous work HIPS[4]. In HIPS the nodes are protected from denial of sleep attack by a hierarchical IPS which uses a Malicious Node Alert (MNA) message system for alerting the nodes to avoid forwarding the packets from the victim node. However, the performance of HIPS may be degraded, when it is applied for a large scale IoT network with multiple BRs. Hence we developed an extended version of HIPS called EXHIPS (Extended Hierarchical Intrusion Prevention System) to detect and prevent the denial of sleep attack for scalable 6LoWPAN networks.

II. Related Works

The denial of sleep (battery drainage) attack is a severe attack in IoT, since recharging or replacing the battery is impossible in a sensordomain. In this attack, the attackerforces the sensor nodes to awake for a longer period of time for nonproductive jobs; so that theenergy of the nodes is exhausted quickly and the network performance will be degraded.According to Stajano et al, there are three different ways of battery drainage attacks found [5]: (i)Malignant attack: application code or kernel binary is adjusted to increase power consumption; (ii) Benign attack: the device is enforced to execute a legitimate but energy-consuming application without changing the application; (iii) Service Request attack: The nodes are repeatedly requested to forward the packets over the network or to find the route etc.,In SVELTE Raza, et al. [6] proposed a hybrid IDS system for IoT, which constructs a network topology at 6BR system to spot the attacks like sinkhole,selective

DOI: 10.9790/0661-180604104108

forwarding and DODAG inconsistency.Chen Jun [7] proposed a real time IDS,whichis working on the basis of Event Processing Model (EPM). It is a rule-based IDS in which rules are stored in Rule Pattern Repository. This approach consumes more CPU resources, and memory to degrade the network performance.In [8] Kasinathan, Prabhakaran, et al. proposed an Intrusion Detection System (IDS) framework for IoTnetworkcreated by 6LowPAN devices. They have created a protocol called DEMO for resource constrained IoT networks, which consists of a monitoring system and a detection engine. Pongle et al.[9]presented amethod, which utilizes the location and neighbor information of a node to recognize the wormhole attack and Received Signal Strength(RSS) to identify attacker nodes.In [10], virtual cluster concept is introduced in which nodes are grouped in the same subnet and shown as a single resource. The WSN is dynamically separated into clusters with separate cluster heads.

III. Proposed Approach

Our proposed method is the fusion of the distributed and the centralized approach. In this method the 6LBR routers are working cleverly such that each 6LBRrouter is acting as avigilant,which can take responsive action, at oncethe detection of malicious activity in the network and immediately alert the other 6LBR routers connected with the same IoT domain by sending the MNA message.

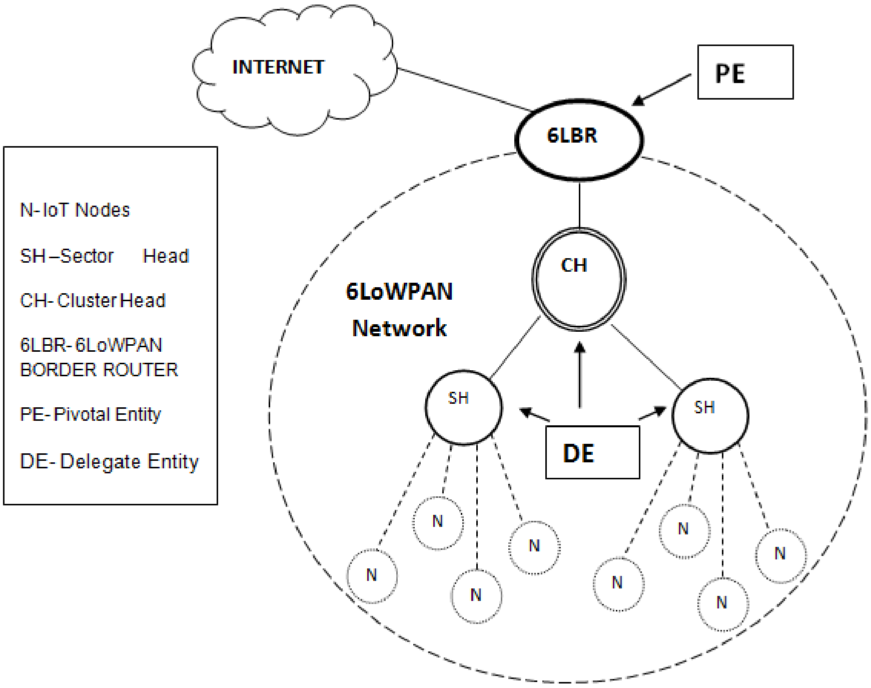

Fig.1. Hierarchical Intrusion Prevention System for IoT

Our basic model HIPS is shown in Fig.1.HIPS consists of the sensor network which is working with 6LoWPAN protocol. The sensor network is separated into possible number of sectors. Each sector is managed by a Sector Head (SH). All the SH nodes are observed by a Cluster Head (CH) and finally this setup is connected to the Internet by means of a 6LBR router.The HIPS system consists of two entities: One is the Pivotal Entity (PE) and the other is the Delegate Entity (DE).The PE is located in 6LBR node whereas the DE is located in SH and CH nodes.In the process of identifying the 'sleep deprivation torture' both the entities functiontogether to efficiently sense the glitches and preclude the network from SD attacks.This is a centralized approach and will be suitable for an IoT under a single 6LBR router.The intended approach is an enhancement and combination of existing two protocols. One is the Gateway Media Access Control (GMAC) [11] which is a centralized protocol and the other is the Collaborative Hierarchical Model (CHM)[12] which uses the distributed approach. Even though these approaches appear to be constructive, they will not be useful for the fast growing IoT on a large scale.Most of the existing IDS techniques are not meant for the requirements for practical deployment in IoT network to overcome sleep deprivation torture.In this section we presented a method, which is a combined approach of both the centralized and the distributed methods. In the centralized method, cluster based mechanism is used in an energy efficient way. Clusters are formed dynamically based on the location and the proximity of nodes. Each cluster has a cluster head (CH) which is acting as server as well as a proxy thus hiding the identity of the sensors[13].

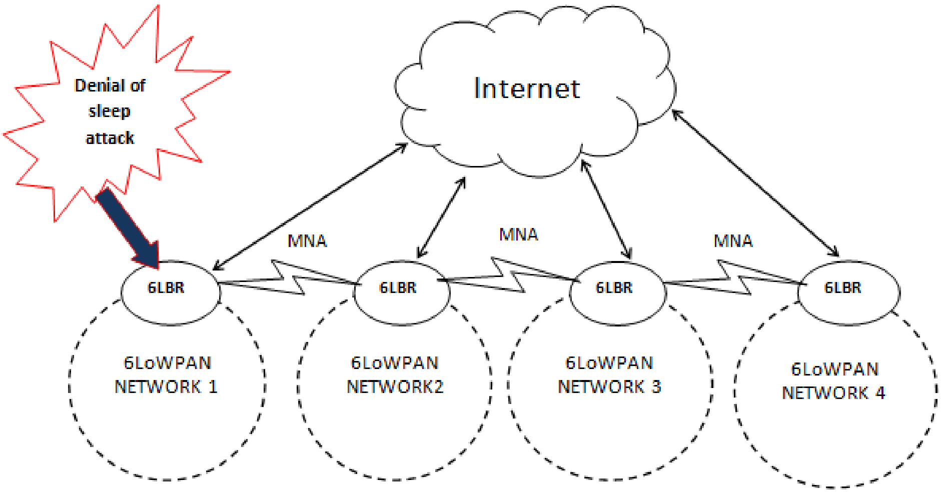

Fig.2. Proposed EXHIPS architecture for using smart routers

Single-hop communication is used at the cluster level whereas multi-hop communication is employed between cluster heads.A self-motivated detection model is designed to overcome the unexpected decease of IDS enabled IoT nodes. Finally the entire 6LoWPAN network is controlled by the 6LBR router which is acting as a gateway to connect with the Internet. In our research we concentrate on distributed anomaly detection technique in order to build a reliable and energy efficient 6LowPAN network.Anomaly is discovered by matching the values with the predefined parameters specified in normal operation. The anomaly detection technique is used to avoid the false intrusion detection. To mitigate the denial of sleep attack, the proposed model physically eliminates the malicious nodes from the network and rejects forged packets.The proposed architecture is shown in Fig.2. Each 6LBR is acting as a Gate Way through which only the 6LoWPAN network is connected to the Internet. In our HIPS the PE element placed in the 6LBR is playing a vital role in detecting the denial of sleep attack. Once an attack is detected, the 6LBR sends a Malicious Node Alert (MNA) message to the CH node. In the proposed EXHIPS, the MNA message is send to the CH node as well as broadcasted to the other 6LBR routers. Since all the 6LBR nodes are connected in multi hop ad hoclink, since the multi hop architecture is has a high energy-efficiency and a high signal to noise ratio and it is naturally functioning in distributed communication [14]. In the distributed communication platform the alert message iscommunicated very fast so that the other interconnected 6LowPAN networks are also protected from the attack. The message format for broadcast MNA is shown in Fig.3.

PAN ID Of sending node 2 bytes	Source Address (1 Byte) (Sending 6LBR node)	Broadcast Address (1 Byte)	Node ID (Affected node) (1 Byte)	Discovered Malicious Node ID (1 Byte)

Fig.3. The MNA message format in the extended IoT domain

IV. Experimental Setup

Our experimental prototype is builtusing Contiki OS with the network simulator cooja. Contiki is an Open Source Operating System for the Internet of Things. Contiki can be used to connect tiny, inexpensive, light weight microcontrollers to the Internet.For the simulation purpose we used the emulated Tmote Sky nodes. The configuration setup is given in table1.

Table.1. Contiki experimental setup

Sl.No	Contiki Configuration	Protocol / Interface
1	Radio Interface	Cc2420
2	Radio Duty Cycling (RDC)	sicslowmac
3	MAC	CSMA
4	Network	Sicslowpan
6	Routing	RPL
7	Transport	UDP

4.1. IDS Energy overhead

In an IoT environment, since the nodes are generally battery powered and energy is a scarce resource, it is advisable to consider the spending of energy in every activity. We make use of the powertrace utility of Contiki to measure the power consumption by our IDS system. Table 2 gives the operating conditions of the Tmote sky nodes.

Table 2. Typical Operating conditions of tmote sky nodes

Sl.No.	Status	Min	Nom	Max	UNIT
1	Supply Voltage	2.1		3.6	V
2	Current Consumption: MCU on, Radio RX	-	21.8	23	mA
3	Current Consumption: MCU on, Radio TX	-	19.5	21	mA
4	Current Consumption: MCU on, Radio off	-	1800	2400	µA
5	Current Consumption: MCU idle, Radio off	-	54.5	1200	µA
6	Current Consumption: MCU standby	-	5.1	21.0	µA

Table 3 provides network model parameters for the Tmote Sky nodes. The system models 50 Tmote Sky nodes and the network lifetimeis based on Tmote Sky power consumption for transmit, receive and for dormant mode operations.

Table 3. Network Model Parameters

Sl.No.	Parameter	Actual Value
1	Number of Nodes	50
2	Effective Data Rate	250 kbps
3	Frame Duration	500 ms
4	Traffic Rate	2 pkts per frame
5	Pay load	64 bytes

4.2. Performance Analysis

In this section we analyze the performance of our proposed HIPS system using the simulation done with cooja simulator in Contiki platform. In our simulation method, we consider the following assumptions for the better understanding. (i)All the IoTnodes are simultaneously installed with new batteries (ii) Nonew nodes are added to the network in the middle of the lifetime. (ii) Network lifetime is defined as the average time between the installation of the network and the time when nodes' power supplies are completely drained.The performance of EXHIPS is evaluated by the averageNode lifetime. Fig.4shows the average life time extended in our EXHIPS method.

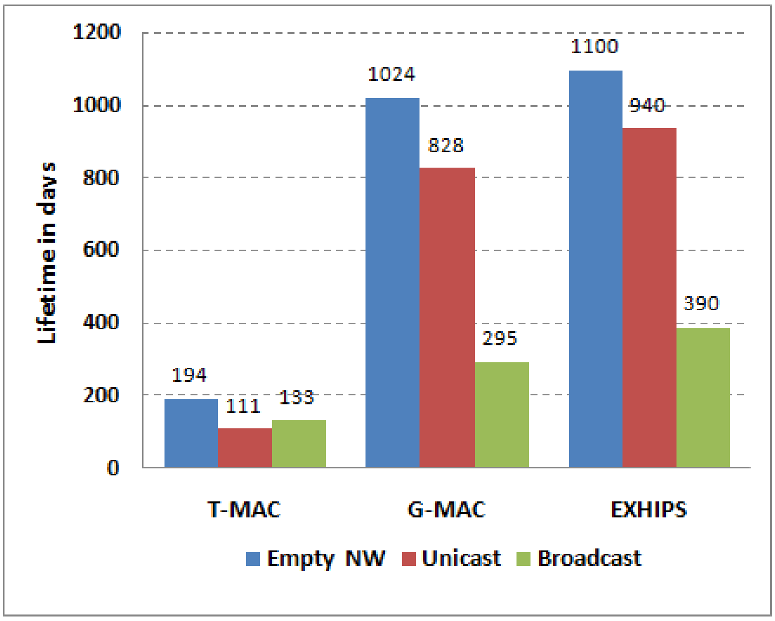

Fig.4. Extension of the average life time by EXHIPS

V. Conclusion and Future work

Since IoT has great and important applications in the near future, it must be protected from various DoSattacks. The Denial of Sleep attack reduces the network life time because of the limited battery power condition. In this work we have designed an architecture which is an extension of our previous workHIPS for detecting and avoiding Sleep Deprivation torture attacks and it isvery much appropriate for resource constrained IoT nodes which runs on 6LoWPAN protocol. Our simulation result proves that his method consumes less energy when a smart IoT application is widened. In future this work can be extended for the other DoS types of attacks in the Internet of Things. We can add the unique Physically Un-cloneable Function (PUF) feature to the nodes in order to detect and prevent the clone ID attack, which improves the security of IoTto a much better level.

References

[1] Deru, Laurent, et al. Redundant border routers for mission-critical 6LoWPAN networks, *Real-world wireless sensor networks.Springer International Publishing,*Vol.281, 2014.195-203.

[2] A.Merlo, M. Migliardi, and L. Caviglione, A survey on energy-aware security mechanisms, *Pervasive Mob.Comput., vol. 24, pp.* 2015, 77–90.

[3] B.Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, Energy Cost of Security in an Energy-Harvested IEEE 802.15.4 *Wireless Sensor Network,* 2014,198–201.

[4] A.Jahir Husain and M.A.Maluk Mohamed, “HIPS: Hierarchical Intrusion Prevention System for Conquering Denial of Sleep Attacks in Internet of Things”, Accepted for publication in Asian Journal of Research in Social Sciences and Humanities (ISSN:2249-7315)

[5] Stajano, Frank, and Ross Anderson. "The resurrecting duckling: security issues for ubiquitous computing." *ComputerVol.* 35(4), (2002): 22-26.

[6] Raza, Shahid, Linus Wallgren, and Thiemo Voigt. SVELTE: Real-time intrusion detection in the Internet of Things,*Ad hoc networks 11(8),*2013, 2661-2674.

[7] Jun, Chen, and Chen Chi., Design of Complex Event- Processing IDS in Internet of Things. *Measuring Technology and Mechatronics Automation (ICMTMA), Sixth International Conference on. IEEE*, 2014.

[8] Kasinathan, Prabhakaran, et al., DEMO: An IDS framework for internet of things empowered by 6LoWPAN, *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM*, 2013.

[9] Pongle, Pavan, and GurunathChavan. Real Time Intrusion and Wormhole Attack Detection in Internet of Things. *International Journal of Computer Applications 121(9)*,2015.

[10] S. Isaiadis and V. Getov, Integrating Mobile Devices into the Grid: Design Considerations and Evaluation, *Proc. of Euro-Par 2005 Conference, LNCS, vol. 3648, , Springer,* 2005. pp. 1080-1088

[11] M. I. Brownfield and N. J. Davis, Energy-efficient Wireless Sensor Network MAC Protocol Energy-efficient Wireless Sensor Network MAC Protocol,” Management, 2006.

[12] T. Bhattasali, Sleep Deprivation Attack Detection in Wireless Sensor Network, *International Journal of Computer Applications, vol. 40, no. 15,* 2012.pp. 19–25

[13] Udoh, Ekereuke, Vladimir Getov, and Alexander Bolotov.Sensor Intelligence for Tackling Energy-Drain Attacks on Wireless Sensor Networks.*Automated Reasoning Workshop,* 2016.

[14] A.K. Singh, S. Rajoriya, S. Nikhil, and T. K. Jain, Design constraint in single-hop and multi-hop wireless sensor network using different network model architecture, *International Conference Computer. Communication Automation*, 2015, pp. 436–441.