International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5| ISSN : 2456-3307

Effective Wormhole Attack Detection and Isolation In 6lowpan Networks

R.Sujatha[1], P.Srivaramangai[2]

[1]Ph.D. Research Scholar,Department of Computer Science, MaruduPandiyar College, Thanjavur , Tamilnadu,India

[2]Associate Professor,Department of Computer Science, MaruduPandiyar College, Thanjavur , Tamilnadu,India

ABSTRACT

Nowadays the improvements in MANET needs for technological enlargement for the efficient data transmission which can be attained throughout the wireless architecture that has its advancements to the core i.e., 6LoWPAN Networks. In common, nearly all the sensors have the ability of communication and the requirement of low power consumption. 6LoWPAN (Low Power Sensor or Mobile devices in IPV6 Network with Gateway) plays a brilliant role in this convergence of heterogeneous technologies thereby permitting sensors to broadcast information using IPv6 stack. Sensors tend to be targets of attacks out of which Wormhole attack is one of the most familiar and threatens the network accessibility by dropping data in between or disturbing routing paths. RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) is a usual routing protocol used in sensor networks and it recommends a RPL-based wormhole detection mechanism. The rank of a node-defined RPL is used to determine the distance through the differences. The proposed detection method determines malicious wormhole nodes if unreasonable rank values are recognized. The experimental results prove that the proposed detection method can identify wormholes effectively under different wireless 6LoWPAN networks.

Keywords :6LoWPAN Networks, MANET, Worm Hole Attack, RPL

I. INTRODUCTION

Wireless sensor networks with IOT (Internet of Things) which is a leading technology, are being applied to various applications such as ecosystem monitoring, disaster watch, building automation, health monitoring, object tracking, and plant control. The vital signals or disaster alerts information's are stored in the sensor data; System malfunctions causes due to transmission failure or error. The existing Internet protocol IPv4 provides only about 4 billion public IP addresses; these IP spaces limit the growth of wireless sensor network applications. IPv6 is the most recent version of Internet Protocol which is a communication protocol that offers a detection and location system for the network devices in the new type of networks. The connectivity and efficient communication capability provided by IPv6 using various sensors and tiny devices.

Here, the network topology may vary due to weak mobility (new nodes join the network or hardware failure of existing devices) or strong mobility (physical movement of nodes) [1]. Topology changes in wireless sensor network causes due to wormhole attack. Therefore, building a security management system is important. The architecture of wireless sensor networks in 6LoWPAN Networks is demonstrated in Fig. 1, where all the sensors transmit data to the root. Figure 2 demonstrates an

example of wormhole where M1 and M2 are two malicious nodes, figure a wormhole tunnel T1 through which redirects the transmissions. Some of the routing paths going through the wormhole tunnel may be shorter than the normal multi-hop routes [2], [3], and [4]. Therefore, wormhole attacks which are the most general attack in this type of network may change the original routing paths, and the wormhole nodes may eavesdrop or discards the data going through the wormhole tunnel.

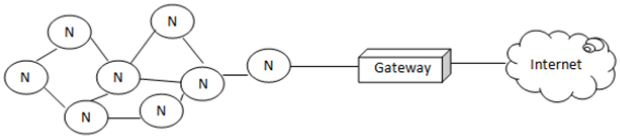

Fig.1. 6LoWPAN Networks

Additionally, the two wormhole end nodes use lot of power energy than others. The sensor network may not operate efficiently, once their resources become exhausted. These kinds of attacks cooperate the network availability and data privacy leading to serious security problems.

In wireless sensor network architecture, each node is only aware of its neighbor nodes and possesses limited resources. Due to the limited computing power capability of the sensor nodes, the centralized and sophisticated detection methods might not be feasible. Also, additional attachment of hardware for all the nodes could make it costly. So, it is practically impossible and costly. Based on the above limitation, this study intend a distributed detection method by applying the standard routing protocol IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), available in all the sensor nodes to recognize wormhole attacks without additional hardware to all the sensor nodes.

RPL [5], [6] is a usual routing protocol for wireless sensor networks [7], which is vulnerable to wormhole attacks [8]. The rank information from RPL utilized in the proposed detection method to calculate approximately the relative distance to the root node; the rank value will be compared with neighbors; if the discrepancy go beyond a threshold value, it signals an anomaly where a wormhole might survive, thereby the attack on the nodes are indentified.

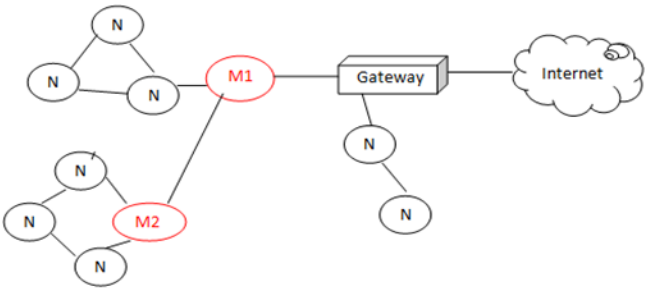

Fig.2 Worm Hole Attack in 6LoWPAN

The main contributions of this paper are as follows:

1. In wireless sensor network, the proposed approach constructs a security mobility management mechanism.
2. Any extra hardware or special powerful nodes does not require as compare to previous [2], [9], [10].
3. The proposed mechanism is depending on an existing protocol. It could also be executed on existing wireless sensor network hardware.
4. Here no centralized analysis is needed due to the proposed mechanism is based on distributed system; Additional communication is not required anymore.
5. The proposed system needs only some computing resource, the lifetime of battery of devices would be left unchanged.

II. RELATED WORKS

In this paper, we propose a wormhole detection mechanism depend on RPL routing protocol. In this section, previous works about detection of wormhole attack are analyzed in Section 2.1. In Section 2.2, we examine the weakness of RPL routing protocol, in addition with some review of RPL-based wormhole detection approaches.

A. Prior work of detecting wormhole attacks

Wormhole attacks in wireless sensor networks were established by Sanzgiri [11], Papadimitratos [12], and Hu [2], [3], [8]. In a wormhole attack, using two malicious nodes wormhole tunnel is constructed. Malicious nodes will "tunnel" their established routing information to another point in the network and then replay them.

Once the wormhole tunnel is constructed, malicious nodes could eavesdrop on traffic from their neighbor nodes, drop packets or to perform man-in-the-middle attacks [4]. Hu et al. proposed two types of packet leashes: such as geographic leashes and temporal leashes to avoid wormhole attacks [4]. Leashes are planned to protect adjacent to wormholes over a single hop wireless transmission. Geographical leash will not pay attention to any messages from unreasonable distance, and temporal leash will ignore any packets with unreasonable lifetime [4]. And, in order to construct packet leashes, all nodes must have synchronized clocks and their own position, which is unreasonable in most wireless sensor network environment.

A lightweight wormhole detection method called LITEWORP was proposed by Khalil et al. [9]. In LITEWORP, each node creates its two-hop neighbor list. By observing all control traffic of neighbor, LITEWORP could determine and separate malicious node. But, monitoring and taking out every neighbor's traffic outcomes in extra overload. Also, it is impossible to identify guard node for particular link. The proposed system is inappropriate for nodes with limited battery capacity. Khalil et al. also proposed a routing protocol called MobiWorp to distinguish and separate wormhole attack [13].

MobiWorp based on a secure central authority (CA) for global tracking of node positions. MobiWorp organized a special node known as guard node to preserve a black list and observe network traffic. But in some wireless sensor network applications is impractical. Choi et al. proposed a Wormhole Attack Prevention (WAP) algorithm which deliberate the round-trip time (RTTs) between neighbors, classifying that two neighbors are not each other's and the communication range are theoretical suffering from wormhole attack [14]. But, WAP algorithm can suitable only for wireless sensor network applications with various nodes and it could not discover false positive alarm, due to limited neighbor nodes' information, the affected nodes have few neighbor nodes.

B. IPv6 Routing Protocol for Low-Power and Lossy Networks

The RPL became a common routing protocol for wireless sensor networks [6]. RPL is mainly designed for 6LoWPAN (IPv6 over Low-powered Wireless Personal Area Networks). Since IPv6 provide lot of IP space, and it suitable for wireless sensor network applications for point-to-point communication or point-to multicast communication among tiny nodes.

6LoWPAN network is a wireless sensor network that supports IPv6. In 6LoWPAN, IPv6 used as Internet layer and IEEE 802.15.4 as data link and as well as physical layer [7]. Dissimilar the typical stand-alone wireless sensor networks, devices of wireless sensor network applications only have few resources, and these devices can be accessed from anywhere. Hence, wireless sensor network applications are showing threats from the Internet and from within the network.

Routing graph information's are exchange by RPL protocol gives new ICMPv6 control messages. For building RPL application information advertised by RPL protocol uses DIO (DODAG Information Objects) messages

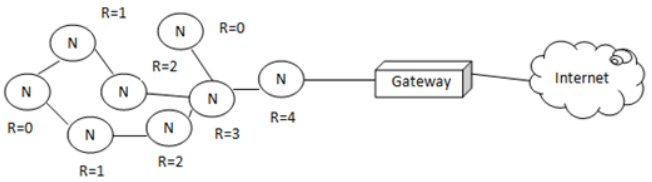

Fig.3. Ranking in RPL

DODAG, and DAO (Destination Advertisement Object) messages are utilized for supporting downward traffic toward leaf nodes. Every interval nodes send DIO and when nodes receive a DIO message, they might use the information to combine a new network or revise their routing table [6]. Now, the most popular wireless sensor network standard supports RPL like ZigBee IP [15, 16].

ZigBee is inexpensive, low-power, wireless sensor network standard which facilitate tiny and smart devices to work jointly for wireless sensor network applications [15]. Therefore, the proposed system will be depending on RPL routing protocol. RPL is also vulnerable to wormhole attack. To construct wormhole tunnel, attackers could send fake ICMPv6 routing packets.

Khan et al. proposed a Merkle-tree-based authentication to avoid wormhole attack [17]. Additionally authentication mechanism was projected while preserving parents within a DODAG can be used for preventing promotion of routes surrounding malicious nodes sending replay attacks around the region. However, building Merkle tree needs additional communication and computation resources again. However, Sensor network applications utilize tiny devices with fewer resources and electricity power. Therefore, additional hardware requirement or complicated detection algorithm is inappropriate for the efficient recognition of wormhole attacks in such environments.

III. PROPOSED FRAMEWORK USING RPL MECHANISM

The proposed system is based on RPL without any extra hardware or difficult detection algorithm. In this paper, an intrusion detection system is proposed to recognize wormhole attacks. To prevent routing loops, the number of hops from a node to the root computed by RPL. In RPL, "Rank" represents the position of a node; when the node moves away from the root, then rank get increases [5].

The geographic leashes [2] cover the way to use node's location to identify wormhole attacks. The distance of root node is estimated by Rank method. Therefore, the rank value is useful in the proposed system to categorize suspicious rank values from DIO messages. To exhibit the idea of the proposed detection method, Figs. 3 and 4 give an example for changing rank values before and after the wormhole tunnel is established. Figure 3 shows the rank.

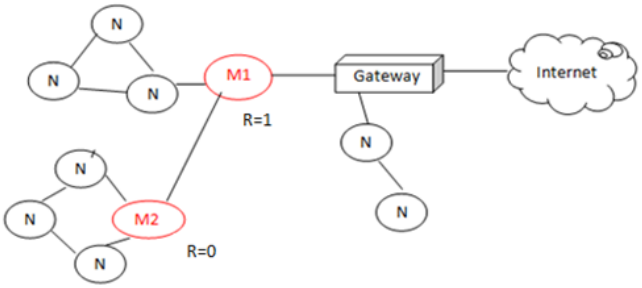

Fig.4. Ranking in Worm hole Attack

RPL define value of each node. If the root node has the rank of 0, then the rank values shows the number of hops to the root plus one. Figure 4 shows the variation of the rank values after the two malicious nodes, M1 and M2, are deployed and create a wormhole tunnel. When the two nodes are introduced in the network, DIO message sends from the root node to node N1 and M1; the rank of node N1 and M1 is 1, to update the routing table.

The DIO message will be broadcasted to the following neighbor nodes to update the rank values. RPL provides the rank value to estimate the distance to the root. The proposed detection method adopts the rank value to classify wormholes. Figure 5 illustrates the framework of proposed system. The RPL specifies four types of control messages for

topology maintenance and information exchange. In this paper, DIO messages are primarily collected by proposed system, and then rank value is taken out from DIO messages. Once DIO messages are taken out, the proposed system will identify if the DIO message is from malicious node or not. The detection algorithm is summarized in Fig. 6. As this is a distributed algorithm, to check if a wormhole exists in the network, each node in the sensor networks systematically observes the features extracted from the packet header. To cut down the detection process, the malicious nodes are stored in a black list once they have been observed.

Proposed Algorithm

Input: Node N, Gateway G, Location Details

Output: Worm Hole attack detection

Algorithm: Proposed RPL Mechanism

[1] Select N Node and Create a WN Network

[2] Find Loc(N) to obtain the location details

[3] Connect foremost N_n node to Gateway g for Internet Connectivity

[4] N_s send RREQ message to the destination node N_d

[5] Find Shortest Routing Path in the network from N_s to N_d

[6] Collect the DIO Messages from the nodes in the routing path

[7] Calculate the Rank R value for the parent to child hierarchy

[8] Find Rank_Threshold R_{Thres} for abnormal DIO messages

[9] R_{Thres} = Rank_Diff($R_{Parent} - R_{child}$)

[10] Check whether R_{Thres} is 1 or not. If $R_{Thres}=1$ then no attack found or else $R_{Thres}>1$ then attack found

[11] Perform these for every node transmission

[12] Isolate through the change in routing path

The rank value from the IPv6 header of an incoming traffic is checked to see if the rank gradually increases or it is different from its neighbors. If the ICMPv6 message is considered as begin, the receivers will inform their neighbor table and routing table correspondingly.

This study imagines that when a wireless sensor network exists, no malicious nodes might arise when it is deployed in the beginning. The correct routing table of each node in the newly deployed network will be recognized before wormhole attack is issued.

The proposed detection method defines the subsequent two attributes to find out abnormal DIO messages: Rank_Threshold and Rank_Diff. Rank_Threshold is distinct as the variation of the rank values between its parent and the node itself as originated in Eq. (1); the attribute value is attained when the routing table is created or updated. For example, as illustrated in Fig. 3, Rank_Threshold of node N5 is 1 because its rank is 5; that of its parent N4 is 4. Therefore, Rank_Threshold of node N5 is $|3 - 4| = 1$.

IV. IMPLEMENTATION RESULTS

The execution has been done in Matlab formed by Math Works for detection of wormhole attacks using proposed mechanism.

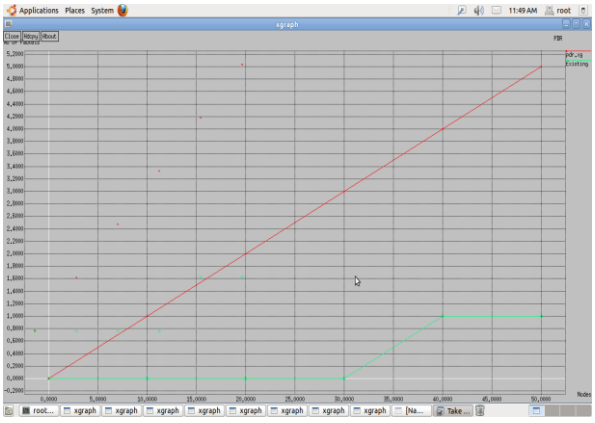

Fig.5.1 Packet Delivery Rate

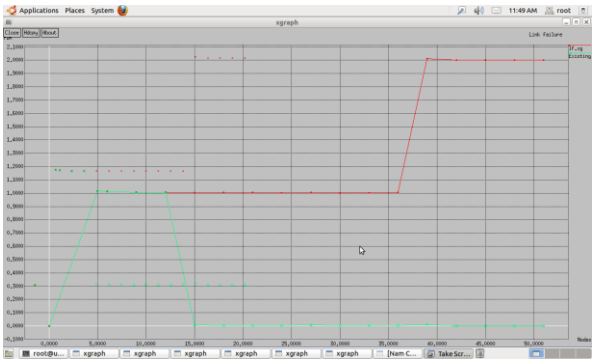

Fig.5.2 Link Delay

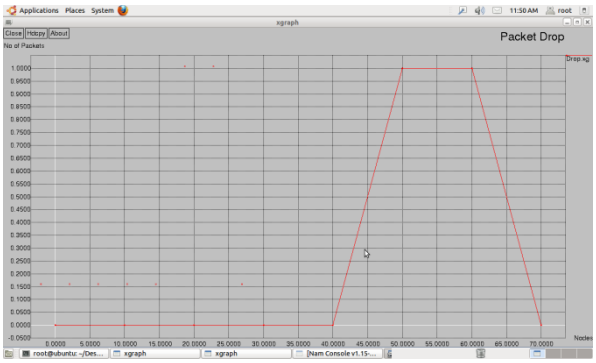

Fig.5.6. Packet Drop

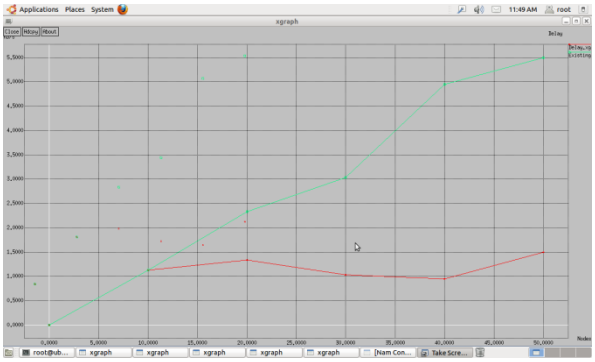

Fig.5.3Packet Delay

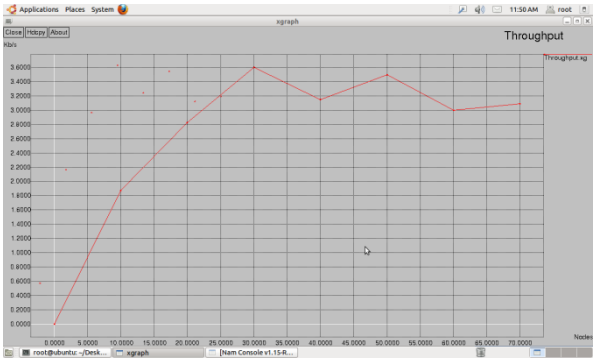

Fig.5.7.Throughput

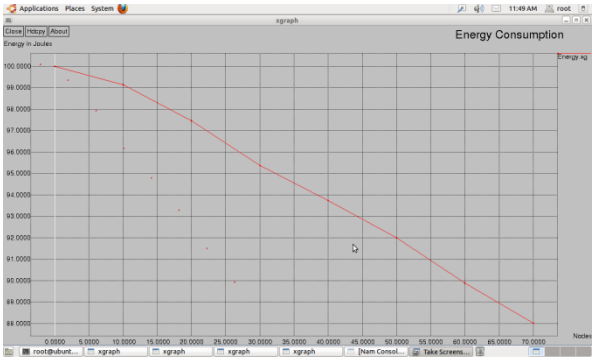

Fig.5.4 Energy Consumption

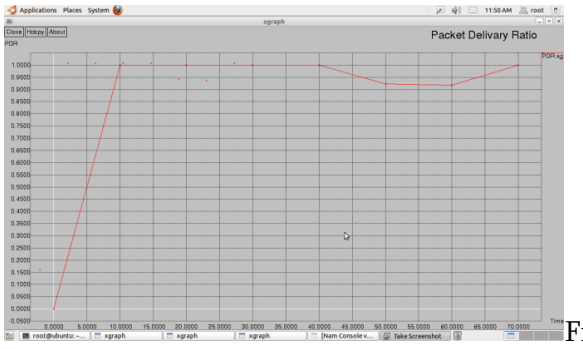

Fig.5.5. Packet Delivery Ratio

V. CONCLUSION

Wireless sensor network or IOT will be the trend as this forming hype around all the fields for many implications. Due to the nature of wireless sensor network, the devices have limited computing and electricity capability. Thus, wormhole detection becomes a challenge in this network. This study proposes a wormhole detection mechanism depended on RPL routing protocol without any extra hardware requirement. The model results show that the proposed system can identify wormhole properly with high efficiency. The proposed detection systems pay attention on the availability of IPv6 wireless sensor network. Malicious nodes can create duplicate DIO messages to avoid detection. Wireless sensor network applications may apply IPSec technology like IPsec-for-6LoWPAN to make sure the privacy and reliability of its applications. The proposed detection system provide a good security mobility management mechanism for wireless sensor network, because (1) the proposed system has 100% accuracy; (2) the proposed system does not need any extra hardware or special nodes; (3) the proposed system

could be applied in any environment; the proposed system needs limited computing resources.

VI. REFERENCES

[1]. M Ali, T Suleman, ZA Uzmi. "MMAC: A mobility-adaptive, collision-free mac protocol for wireless sensor networks," in Performance, Computing, and Communications Conference, 2005. IPCCC 2005. (24th IEEE International, Phoenix, 2005), pp. 401-407

[2]. L Hu, D Evans. "Using Directional Antennas to Prevent Wormhole Attacks," in NDSS, (San Diego, 2004)

[3]. Y-C Hu, A Perrig, DB Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks," in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. (IEEE Societies, San Francisco, 2003), pp. 1976-1986

[4]. Y-C Hu, A Perrig, DB Johnson, "Wormhole attacks in wireless networks," Selected Areas in Communications. IEEE J 24, 370-380 (2006)

[5]. T Tsvetkov, RPL: IPv6 routing protocol for low power and lossy networks. Sens Nodes Oper Netw Appl 59, 2 (2011)

[6]. T Winter, "RPL: IPv6 routing protocol for low-power and lossy networks". 2012

[7]. L Wallgren, S Raza, T Voigt. "Routing Attacks and Countermeasures in the RPL-based Internet of Things," International Journal of Distributed Sensor Networks, vol. 2013, 2013. http://dsn.sagepub.com/content/9/8/794326.full

[8]. O Garcia-Morchon, S Kumar, R Struik, S Keoh, R Hummen, Security Considerations in the IP-based Internet of Things, 2013

[9]. I Khalil, S Bagchi, NB Shroff, MOBIWORP: mitigation of the wormhole attack in mobile multihop wireless networks. Ad Hoc Netw 6, 344-362 (2008)

[10]. R Poovendran, L Lazos, A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Netw 13, 27-59 (2007)

[11]. K Sanzgiri, B Dahill, BN Levine, C Shields, EMB Royer. "A secure routing protocol for ad hoc networks," in Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, Paris, 2002, pp. 78-87

[12]. P Papadimitratos, ZJ Haas, Secure Routing for Mobile Ad Hoc Networks (the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, 2002), pp. 193-204

[13]. I Khalil, S Bagchi, NB Shroff. "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," in Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, Yokohama, 2005, pp. 612-621

[14]. S Choi, D-y Kim, D-h Lee, J-i Jung. "WAP: Wormhole attack prevention algorithm in mobile ad hoc networks," in Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC-08. (IEEE International Conference, Taichung, 2008), pp. 343-348