www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 12 Dec. 2016, Page No. 19358-19362

Deist: Dynamic Detection Of Sinkhole Attack For Internet Of Things

R. Stephen, A. Dalvin Vinoth Kumar, Dr. L. Arockiam

Research scholar
Dept. of computer science St. Joseph's college(Autonomous)
Tiruchirappalli-620002
Stephenr1989@gmail.com
Research scholar
Dept. of computer science St. Joseph's college(Autonomous)
Tiruchirappalli-620 002
dal_win@ymail.com
Associate professor
Dept. of computer science St. Joseph's college(Autonomous)
Tiruchirappalli-620 002
larockiam@yahoo.co.in

Abstract: **The Internet of Things (IoT) interconnects things, human and animals into a single network. The devices connected in IoT are light weight devices. The security for light weight IoT device is a challengeable task. It faces the vulnerabilities in communication infrastructure due to the different attacks. The attacks are selective forwarding attack, sinkhole attack, black hole attack, Sybil attack, wormhole attack etc. The sinkhole attack is one of the most destructive routing attacks in IoT environment. A sinkhole attacker aims to attract the greatest amount of traffic in a given area and harms the reception of data on collection point. The proposed method is an active detection of sinkhole attack. It uses the Alternative Parent (AP) information to identify the attacker. This method provides security to IoT network from unwanted traffic created by the attacker node.**

***Keywords - IoT security, Sinkhole attack, 6LowPAN, Routing attacks, RPL*.**

I. INTRODUCTION

The Internet of Things (IoT) is the next evolution of internet. It is adopted with people and things or objects. Internet is not only adopted by people but also by devices [1]. The main objective of the Internet of Things is connecting more devices and it is expected to connect over 50 billion devices by 2020 [2]. Internet of Things is a heterogeneous network that integrates devices named smart objects, appliances, books, cars, computers, sensors, smart phones, PDAs, other devices. These devices share information, data and resources over the network. Also, IoT has a number of application domains, such as college management system [3] in education and also in healthcare, environment, logistics, agriculture and many others.

The Routing Protocol for Low-power and Lossy networks (RPL) is recently standardized routing protocol for the IoT. RPL is primarily designed for Low-power and Lossy Networks (LLNs), also called IPv6 over Low-powered Wireless Personal Area Networks (6LoWPAN). Providing security in IPv6/RPL connected 6LoWPANs is challenging because the devices are connected to the untrusted internet and are resource constrained [4].

The deployment of the IoT requires secure communication which is a challenge because of the heterogeneity of the IoT devices. The communication between the IoT devices should be secured end to end. Secure communication means that confidentiality and the integrity of messages should be enforced between the source and the destination. Though message security provides confidentiality and integrity of data packets in transit and authentication between devices, an attacker can still launch a number of attacks against the IoT [5].The remaining of this paper organized as follows. Section II discusses some of the related attacks and techniques. Section III gives a brief explanation of the proposed work. Finally, section IV concludes the paper.

II. RELATED WORKS

Cervantes et al. [6] proposed an intrusion detection system called INTI (Intrusion detection of sinkhole attacks on 6LoWPAN for internet of things). This system used to identify sinkhole attacks on the routing services in IoT. The system combines watchdog, reputation and trust strategies for detection of attackers by analyzing the behavior of devices. The results showed that INTI performance and its effectiveness in terms of attacks detection rate, number of false positives and false negatives.

Dhumane et al. [7] surveyed the most important aspects of routing in IoT. This survey emphasized on routing of the data in IoT. The author analyzed and consolidated the past research work.

Wallgren et al. [8] provided a comprehensive analysis of IoT technologies and their new security capabilities that could be exploited by attackers or IDSs. This paper measured the routing attacks in the RPL based Internet of Things in 6LoWPAN networks. It measured the various routing attacks against RPL. One of the main contributions of this paper is the implementation and demonstration of well-known routing attacks against

6LoWPAN networks running RPL as a routing protocol for everything running on Internet [9].

John et al. [10] discussed the different security attacks like selective forwarding, sinkhole, sybil and blackhole with their impact on the routing protocols. This article emphasized on reviewing the effects of network layer attacks on routing protocols in wireless sensor networks. Also, there are many other attacks detected and solutions are proposed. Some of them are tabulated in Table 1.

Table 1.Attacks and Techniques

Author name	Title	Attacks	Technique
Pongle [12]	Real Time Intrusion and Wormhole Attack Detection in Internet of Things	Wormhole Attack	SAM
Kumar [13]	Routing Attacks and Countermeasures in the RPL-based Internet of Things	Clone Id and Sybil attack	DHT
Chiu[14]	DelPHI: wormhole detection mechanism for ad hoc wireless networks	Wormhole attacks	DelPHI
Dhurandher [15]	E2siw: An energy efficient scheme immune to wormhole attacks in wireless ad hoc networks	Sinkhole and wormhole attacks	E2siw
Ngai [16]	On the intruder detection for sinkhole attack in wireless sensor networks	sinkhole attack	Network Flow

Nguyenet al. [11] proposed the intrusion detection system for the IoT called SVELTE. IoT things are connected with unreliable and untrusted internet via IPv6 and 6LoWPAN networks. So, these things are exposed to wireless attacks inside the 6LoWPAN networks. To handling these attacks, intrusion detection systems are necessary. This paper designed, implemented and evaluated the intrusion detection system to detect the routing attacks such as spoofed or altered information, sinkhole and selective forwarding.

III.PROPOSED WORK

The proposed work is to detect the sinkhole attack in the IoT network.RPL is one of the popular routing protocol for IoT. In RPL, the sink node act as the border router. Storing and non-storing are two types of RPL. The nodes in RPL construct the Destination Oriented Directed Acyclic Graph (DODAG). The nodes choose their parent node by the rank value. The value of the rank is constantly increased in downwards and vice versa. The sink node is the router node, P is the parent node, and S is the child node as show in Fig 1. In proposed work, there are three main phases involved (i) DODAG construction, (ii) Detection and (iii) Sinkhole treatment

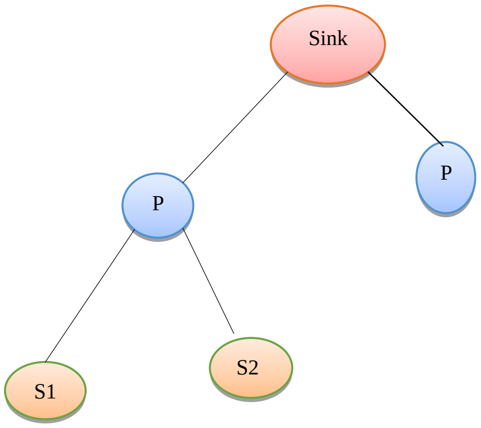

Fig. 1: IoT node distribution

A. Construction:

In the construction phase, the sinkhole node acts as a leader node and initializes the construction request. The request is broadcasted to the neighbors. When a node receives the construction request, it will send a response acceptance if and only if the node doesn't have any parent. In case, a node is already part of a network, then the current rank and received rank are compared. The lower rank is selected as the parent. As shown in Fig. 2a the old node belongs to the DODAG-1. The new node broadcast the construction request packet. The node S doesn't have any parent node, so accept the request and join with the new node and forms the DODAG-2.

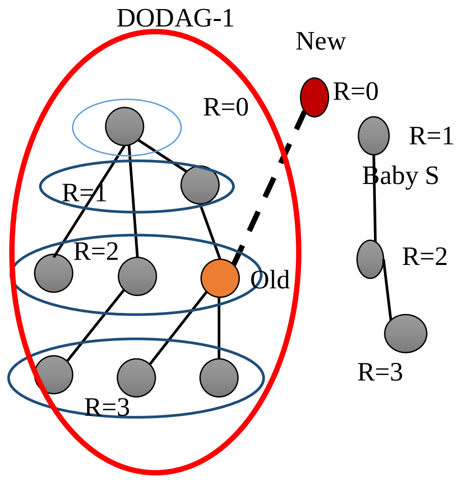

Fig. 2a: DODAG Construction

The old node also receives the request and compares the rank value with its own parent node. The rank of old node parent is 1 as shown in Fig. 2a. The rank of new request is 1 as shown in Fig. 2b. The old node disconnects the connection from DODAG-1 and joins the new network DODAG-2.

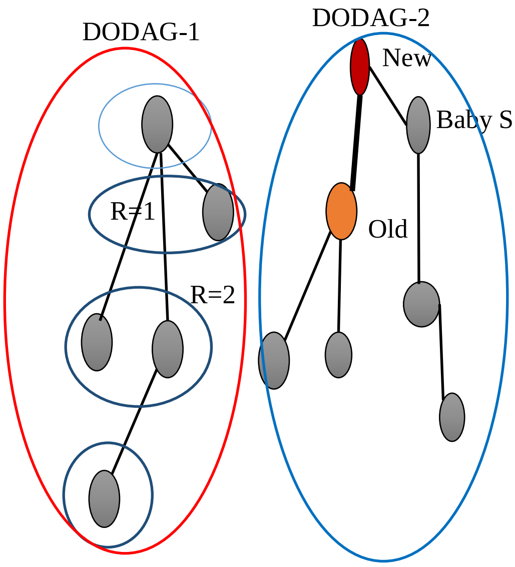

Fig. 2b: DODAG Establishment

B. Detection phase:

In wireless low power network, each and every node acts as router as well as sender. These types of networks are easily vulnerable by attacks like sinkhole attack. The attacker node announces the fake path towards the sink node. The proposed work includes the detection phase to detect these kinds of attacker nodes.In the network scenario as shown in Fig. 3 the node S_2 can communicate with both P and AP. The objective function (OF) of P is optimum towards the sink node for the node S_2. The node S_2 chooses the node P as the parent node. The node AP acts as the alternative parent node for S_2. Whenever the node S_2 wants to send the data to the sink node and the parent node is valuated. The OF between S_2 to sink, P to AP and S to AP are used to detect the sinkhole node. Once the attacker node I detected, it will be published in the network to other nodes. The detection mechanism is explained in the following algorithm. The variables used in the technique are listed below.

S-sink node
P-Parent node
AP-Associated Parent node
N-Node list
CRP-Construction of Request Packet
P- Parent
AP - associate parent
Distance of sink to AP is d_{AP}
Distance of sink to P is d_P
Distance of sink to n is d_n
Distance of d_P *and* d_{AP}*is* d_{APP}
+ve – positive
-ve- Negative
A - Attacker node
A_c *– Attacker correctly identified*
N – Number of iteration
N = (d,c)
d - Detection performed
c - Current relationship of node n_i

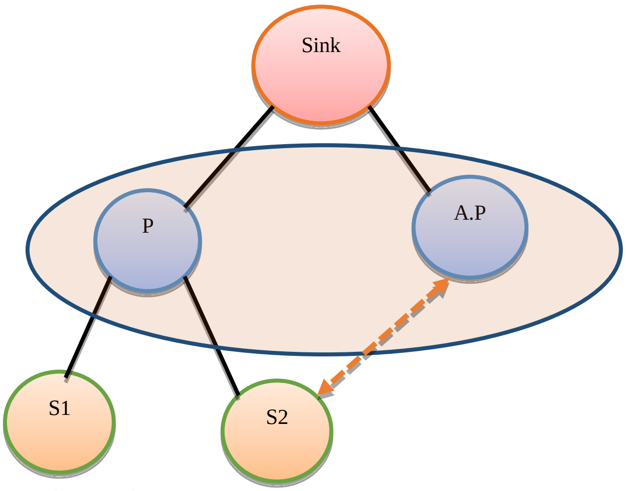

Fig 3: Sink Attacker Detection

```
Phase 1:
    DODAG construction ();
    {
        Construct CRP;
        Broadcast the CRP;
    While (1)
        {
            Parent== i;     i= 0 =accept,
    i=1=discard
    }
    Choose the parent node to establish the network:
    Associated parent (AP) update its routing table;
    }
Phase 2:

        Detection ()
        {
                Node (n) initialize the path discovery;
        n receives j possible paths towards the sink
        Validate the path();
        Rank(p)=rank(AP)

        Route_1 N→P→S
        Route_2 N→AP→S
        Reference route_1
        S→ AP → P → Sink
        Reference route_2
        S → P → AP → Sink
        S → AP = X
        S → P = Y
                If
                Reference route_1  ≥ Reference route_2
                then
                Discover the new parent node;
                Else
                        Transfer the data;
                }
Phase 3:

         Sinkhole elimination ()

         {
```

If (Sinkhole node = = j)

$$Where \begin{cases} j = 1(True) \\ j = 1(True) \\ . \end{cases} \qquad (1)$$

Publish the sinkhole node in the network;

}

The possibility of attacker node for different scenarios is calculated. The number of attacker nodes are formulated using the normal distribution as shown in the Fig 4.The request identified in the detection phase falls into four categories

- Sinkhole node (true)& Correct parent node (False)
- Incorrect sinkhole (False +ve)
- Incorrect sinkhole (False –ve)

i. Sinkhole node (true)& Correct parent node (False)

The sinkhole node (A_c) is the number of attacker nodes identified correctly. This value is achieved by the equation 1. The amount of period the attacker node identified as a true attacker. Where,

$$A_c = \frac{\sum di}{|N|}$$

$$Where \begin{cases} di = ci = 1 \\ di \neq ci = 0 \\ . \end{cases} (1)$$

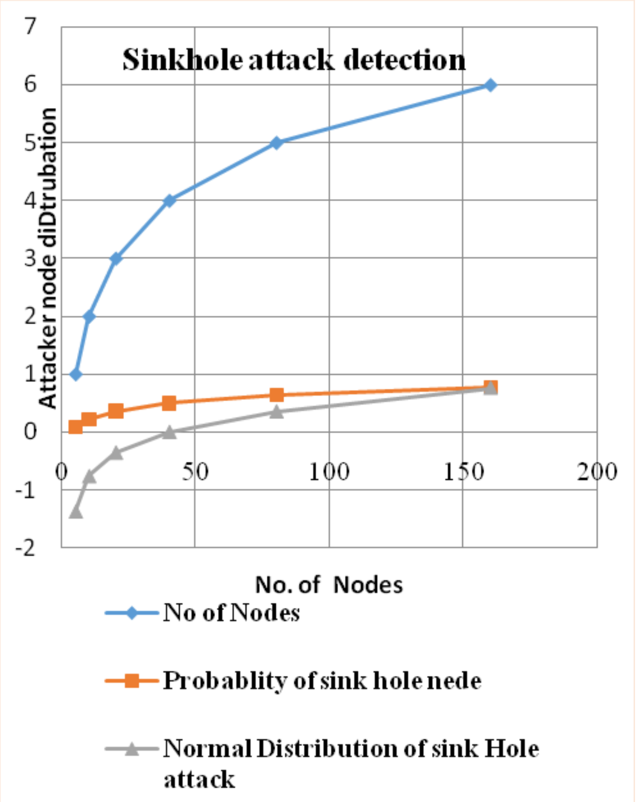

Fig 4: Distribution of sinkhole attack vs Total No of nodes

ii. Incorrect sinkhole (False –ve)

The incorrect sinkhole false - ve (AF_n) is the amount of period the attacker node consider as a trusted node. It is achieved by equation 2.

$$AF_n = |N| - A_c \qquad (2)$$

iii. Incorrect sinkhole (False + ve)

The attacker node (A_c) is detected and it is achieved by the amount of attacker detected in a set of node n_i with amount of period the attacker node consider as an attacker. The incorrect sinkhole false + ve is achieved by equation 3.

$$AF_p = \frac{\sum dni}{|N|} dn_i = \begin{cases} di = ci = 1 \\ di \neq ci = 0 \end{cases} \qquad (3)$$

IV. CONCLUSION

The proposed method is a technique that is used in detection of sinkhole attack. The existing techniques like watchdog are not adaptable for IoT network. Active detection mechanism is used to detect sinkhole attack dynamically. The reference of Alternative Parent (AP) is taken into account for detection of sinkhole node. The results are categorized into four types of outcome using the probabilistic normalization method. The proposed method gives low rate false positive and false negative. In the future, the proposed method needs to be simulated with cooja simulator and results are to be examined under different network topology circumstances.

REFERENCES

[1] Viller, S., Worthy, P., Bodén, M., Weigel, J., Fitzpatrick, G., Rodden, T., & Matthews, B. “IoT: Designing for Human Values”, In Proceedings of the 2016 ACM Conference Companion Publication on Designing Interactive Systems, 2016, pp. 61-64.

[2] Hammon, Jasmin. "Alterity and freedom of information on the internet: the loss of net neutrality in contemporary literature", ACM SIGCAS Computers and Society vol.45, no. 3, 2016, pp.91-99.

[3] A. Dalvin V.K, S. Santiago and Dr. L. Arockiam, “QRIC: QOS Aware routing for internet of things in college management system”, IJERT, 2016, pp. 38-40.

[4] Chandra, TejBahadur, PushpakVerma, and A. K. Dwivedi. "Operating Systems for Internet of Things: A Comparative Study", Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. ACM, 2016.

[5] Mun, D. H., Le Dinh, M., &Kwon, Y. W,“An Assessment of Internet of Things Protocols for Resource-Constrained Applications”, InComputer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual Vol. 1, 2016, pp. 555-560.

[6] C. Cervantes, D. Poplade, M. Nogueira and A. Santos, “Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things”, International symposium on integrated network management (IM2015), 2015.

[7] A. Dhumane, R. Prasad and J. Prasad, “Routing issues in Internet of Things: A Survey”, proceedings of the international conference of engineers and computer scientists 2016, vol. 1, IMECS, March 2016.

[8] L. Wallgren, S. Raza and T. Voigt, “Routing attacks and countermeasures in the RPL-based Internet of Things”, International journal of distributed sensor networks, article ID 794326, volume 2013.

[9] Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "Secure routing for internet of things: A survey", Journal of Network and Computer Applications, (2016): 198-213.

[10] C. John, C. Wahi, “Vulnerabilities of routing protocols in wireless sensor networks”, international journal of advanced research in computer and communication engineering, vol.5, issue.2, February 2016.

[11] K.T. Nguyen, M. Laurent, N. Oualha, “Survey on secure communication protocols for the Internet of Things”, international journal of ad hoc networks, Elsevier, 2015.

[12] Pongle, Pavan, and GurunathChavan. "Real Time Intrusion and Wormhole Attack Detection in Internet of Things", International Journal of Computer Applications 121.9 (2015).

[13] Kumar, S. A., Vealey, T., & Srivastava, H. “Security in Internet of Things: Challenges, Solutions and Future Directions”, 49th Hawaii International Conference on System Sciences (HICSS) 2016. pp. 5772-5781

[14] Chiu, Hon Sun, and King-Shan Lui. "DelPHI: wormhole detection mechanism for ad hoc wireless networks", 2006 1st International Symposium on Wireless Pervasive Computing. IEEE international conference, 2006.

[15] Dhurandher, Sanjay Kumar, et al. "E2siw: An energy efficient scheme immune to wormhole attacks in wireless ad hoc networks", Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on. IEEE, 2012.

[16] Ngai, Edith CH, Jiangchuan Liu, and Michael R. Lyu. "On the intruder detection for sinkhole attack in wireless sensor networks", 2006 IEEE International Conference on Communications. Vol. 8. 2006.