An Enhanced Technique to Detect Sinkhole Attack in Internet of Things

R. Stephen
Research Scholar, Department of Computer Science
St. Joseph's College (Autonomous)
Tiruchirappalli, Tamilnadu, India.

Dr. L. Arockiam
Associate Professor, Department of Computer Science
St. Joseph's College (Autonomous)
Tiruchirappalli, Tamilnadu, India.

***Abstract*— Internet of Things (IoT) has enabled with more heterogeneous devices. These devices are communicate together with wireless sensor network. IoT provides a system for the monitoring and controlling of the physical devices. Hence, IoT devices are called as nodes. These nodes are capable of the collection, processing and analysis of data by IoT sensor devices in the network. IoT network is facing different routing attacks. Such as selective forwarding, sinkhole, Sybil, wormhole etc. This paper deals with the sinkhole attack in IoT network and uses watchdog technique to detect sinkhole attack in internet of things environment.**

***Keywords*— IoT, routing attacks, watchdog, Sinkhole attack**

I. INTRODUCTION

This section describes the basic concepts of proposed work.

A. Internet of Things

Internet of Things (IoT) is the next evolution of internet. It is connecting with huge number of heterogeneous devices. IoT uses different terminologies for its deployment. IoT devices are sensor based and communicate together. Hence, the usage of IoT applications are rapidly growing day by day. But, the deployment of IoT applications is a challenge due to security problem [25]. Because, IoT devices are constrained due to limited power, storage and energy. Security is one of the hot topic in research area. Mostly, routing attacks are occurred in internet of things environment. In existing system, security solutions and approaches are not sufficient one. This paper used watchdog mechanism to detect the sinkhole attack in IoT environment.

B. Sinkhole Attack

Among other routing attacks, sinkhole attack is the most destructive routing attacks in IoT environment. It creates the network traffic and collapses the network communication. It used different routing metrics. The metrics are fake link quality, shortest path etc. Sinkhole attack creates the fake information and sends the route request to neighbor nodes. This attack compromised the nodes.

C. Watchdog Mechanism

This paper uses the watchdog strategy to detect sinkhole attack. Watchdog mechanism is a kind of behavior monitoring system which is the base of trust systems in wireless sensor network. It is one of the intrusion detection techniques which detects the misbehaving nodes in the network.

II. RELATED WORKS

In related works, several papers proposed different mechanisms for Internet of Things security. Most of the papers used the Intrusion Detection System (IDS) to solve the routing attacks. There are different types of routing attacks. Such as selective forwarding attacks, Sybil attacks, wormhole attacks, sinkhole attacks etc. Comparatively, a sinkhole attack is one of the most destructive routing attacks in Internet of Things. This section explains the different author's mechanisms and declarations.

Saoreen et al. [18] used Neuro-fuzzy algorithm with Sugeno fuzzy rules to handled Phy/Mac layer attack in network. This algorithm checked the network either genuine or attack. Shahid et al. [19] proposed SVELTE intrusion detection system to detect routing attacks. Linus et al. [1] proposed the Intrusion detection system with novel security mechanism. It measured the routing attacks in the RPL. Tariqahmad et al. [2] analyzed data security and routing layer security.

Shaker et al. [4] described secure routing protocol called PASER against DoS attacks. It used ambient assisted living applications. Anass et al. [5] used the key management and IDS system to solve the 6LoWPAN layer attacks. The paper analyzed the security aspects in 6LoWPAN network.

Bull peter et al. [6] proposed Open flow control and pox controller to solve TCP/ICMP flow based attacks. Particularly, the paper provided security for IoT devices using an SDN gateway. Christian et al. [7] proposed Intrusion detection system to identify sinkhole attacks on 6LoWPAN networks for IoT. Mohamed et al. [8] used the Intrusion detection system with signature based technique. The paper illustrated IDS against sinkhole attack in WSN with mobile sink.

Anthea et al. [9] classified the routing attacks against network resources, topology and traffic. The paper used taxonomy architecture for RPL networks. Hamed et al. [10] used the web mining technique and fuzzy logic approach to detect Denial of Service attacks.Vin la et al. [11] expressed Intrusion detection system and algorithm to detect misbehavior node in 6LoWPAN. Pavan et al. [12] analyzed the various routing attacks on RPL and 6LoWPAN. Kashif et al. [13] proposed a new protocol called RAEED to detect sinkhole attacks and DoS attacks.

This protocol had able to address the problem. Jorge et al. [14] summarized different mechanisms for communication security in 6LoWPAN and RPL. Surendar et al. [15] used IDS, INTI, IDRS and constrained based technique to detect sinkhole attack.

Viki et al. [16] used anomaly based detection system to detect wormhole attack. This paper developed a tool for exposing security threads in IP-enabled WSN. Ibrahim et al. [24] presented a mechanism to detect sinkhole attack using hop count technique in WSN. Fang-jiao zhang et al. [19] proposed redundancy mechanism to detect sinkhole attack in WSN based on the multipath selection. This paper used dijkstra algorithm to calculate the shortest path. Vijay et al. [23] presented traffic analysis tool to identify attacks against RPL in 6LoWPAN.

III. MOTIVATION

As related works stated that Internet of Things is becoming an emerging technology widely. Internet of Things connected with huge number of devices. Hence, communication among IoT sensor nodes is an important aspects. But security is one of the big challenge in internet of things. Especially, data security plays an important role in network. But, IoT is facing different types of routing attacks due to constrained devices. However, IoT needs an efficient security solution for communication aspects.

IV. OBJECTIVE

The objective of this paper is to detect sinkhole attacks in wireless sensor networks for internet of things. This paper is used watchdog mechanism to analyze the behavior of the nodes. This mechanism is based on Trust and reputation strategies. It uses link quality as a parameter.

V. PROBLEM STATEMENT

Internet of Things is connecting with heterogeneous devices and communicate with together. Hence, IoT adopts machine to machine communication. These devices are deployed in an open place. But, IoT devices are constrained due to limited power, storage and energy. The intruder launch the different routing attacks due to constrained devices. In existing system, the proposed methods and approaches were not fulfilled the security solution.

IoT sensor nodes are affecting with different routing attacks. Routing attacks are sinkhole, selective forwarding, Sybil, Denial of Service, wormhole etc. Among other routing attacks, sinkhole attacks is one of the dangerous one. It creates the fake information and send it to other compromised nodes. In fig 1. Shows that the activity of sinkhole attack.

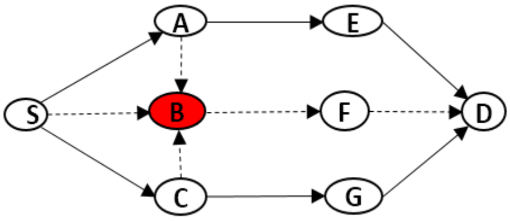

Fig 1. Sinkhole Attack (node B)

In figure 1. S is the source node, D is the destination node and A, B, C, E, F and G are relay nodes. Here, node B is the sinkhole attacker node. It receives data packets from nodes S, A, B and C and not send the data packets to the destination. Sometimes, it acts like selective forwarding attack that is attacker node drops the data packets and send the remaining data packets.

VI. PROPOSED METHOD

The proposed method is used to identify the sinkhole attack in internet of things environment. This paper used watchdog mechanism to detect the sinkhole attack. Watchdog is one of the intrusion detection technique in wireless sensor network. It is a monitoring technique which detects the misbehaving nodes in the network. In this work, watchdog method creates a table to store the behavior of the nodes. Each node maintains the temporary data of neighbor nodes.

Scenario 1:

In fig 2. Shows that the successful data transmission between source to destination.

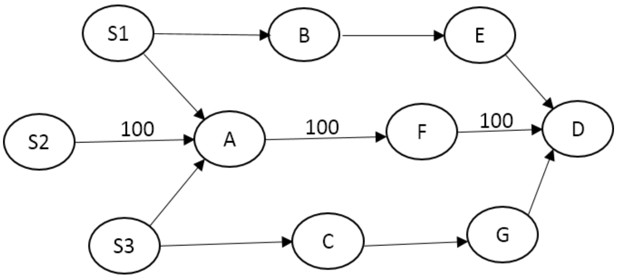

Fig 2. Successful data transmission between S2 to D

As shown in fig 2. S1, S2, S3 are source nodes, D is the destination node and nodes A, B, C, E, F, and G are relay nodes and communicate within range. Source node S2 sends the data packets to the destination node D. Here, node A and node F are intermediate nodes which send all the data packets to the destination node. The successful data transmission is denoted as:

S2→A→F→D

In table 1. Shows that the watchdog method table which is monitoring the behavior of nodes. This method used link quality as a parameter. Finally, it shows the status of the link.

Table 1. Watchdog strategy for one link

Node_Id	No.of packets send	No. of packets received	Link status
S2	100	100	Success

Scenario 2:

In fig 3. Shows that two failure links. These two links send the data packets to the destination, but destination node D not received all the data packets. Here, sinkhole attack node A drops the data packets.

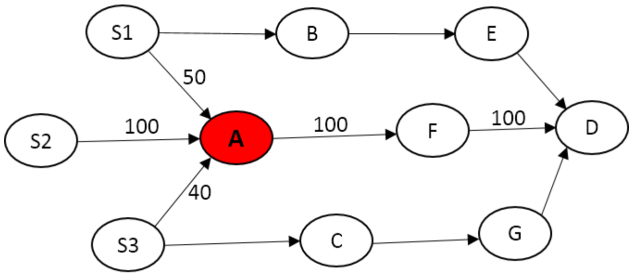

Fig 3. Data packets dropped by sinkhole node A

As shown in fig 3. S1, S2, S3 are source nodes. Source node S2 sends the data packets to the destination node D and it received all the data packets successfully. Similarly, source node S1 and S3 are sending the data packets to the destination node D but it is not received all the data packets. In this case, sinkhole node A dropped the packets. Hence, node A received the data packets from three source nodes S1, S2 and S3. Among three source nodes, node S2 is only successfully send the data packets. The data flow of above scenario is denoted as:

Link 1: S1→A→F→D→Failure
Link 2: S2→A→F→D→Success
Link 3: S3→A→F→D→Failure

Table 2. Describes the watchdog monitoring table. This table concludes the number of successful link.

Table 2. Watchdog monitoring for three links

Node_Id	No.of packets send	No. of packets received	Link status
S1	50	0	Failure
S2	100	100	Success
S3	40	0	Failure

Scenario 3:

This scenario describes the three successful link ratio. For example fig 4. Shows that source nodes S1, S2 and S3 are successfully send the data packets to the destination. In this case, watchdog mechanism is analyzing the behavior of the nodes and send the response to the neighbor nodes.

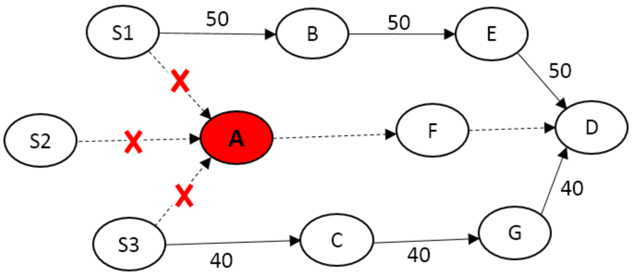

Fig 4. Successful link quality

Now, source nodes are received the response from other neighboring nodes by using watchdog mechanism. These source nodes are analyzing the response and choose the best link for sending data packets. Watchdog mechanism is deployed in each nodes. It is monitoring the behavior of neighbor nodes which detects the malicious node in network.

IV. CONCLUSION

Many researchers proposed different techniques to detect sinkhole attack with various routing parameters and metrics. This paper used successful link ratio as a parameter. The proposed technique used the watchdog mechanism to handle the behavior of a node. This mechanism analyzes the number of links data packets are successfully send or not. This paper concentrates only on sinkhole attack. In future, the proposed mechanism will be applied to different routing attacks with various parameters and implementation.

REFERENCES

[1] Wallgren Linus, Shahid Raza, and Thiemo Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things", *International Journal of Distributed Sensor Networks*, 2013.

[2] Sherasiya Tariqahmad, Hardik Upadhyay, and hiren b. patel, "A survey: Intrusion detection system for internet of things", *International journal of computer science and engineering*, Vol. 5, Issue 2, pp. 81-90, 2016.

[3] Farooq M. U., Muhammad Waseem, Anjum Khairi, and Sadia Mazhar, "A critical analysis on the security concerns of internet of things (IoT)", *International Journal of Computer Applications*, vol.111, no.7, 2015.

[4] Alanazi Shaker, Jalal Al-Muhtadi, Abdelouahid Derhab, Kashif Saleem, Afnan N. AlRomi, Hanan S. Alholaibah, Joel J.P.C Rodrigueset, "On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications." *E-health Networking, Application & Services (HealthCom), 2015 17th International Conference on*. IEEE, 2015.

[5] Rghioui Anass, Mohammed Bouhorma, and Abderrahim Benslimane, "Analytical study of security aspects in 6LoWPAN networks", *Information and Communication Technology for the Muslim World (ICT4M), 2013 5th International Conference on*. IEEE, 2013.

[6] Bull Peter, Ron Austin, Evgenii Popov, Mak Sharma, and Richard Watson, "Flow Based Security for IoT Devices Using an SDN Gateway", *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on*. IEEE, 2016.

[7] Cervantes Christian, Diego Poplade, Michele Nogueira and Aldri Santos, "Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things," *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*. IEEE, 2015.

[8] Guerroumi Mohamed, Abdelouahid Derhab, and Kashif Saleem, "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink", *Information Technology-New Generations (ITNG), 2015 12th International Conference on*. IEEE, 2015.

[9] Mayzaud Anthéa, Rémi Badonnel, and Isabelle Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", *International Journal of Network Security*, Vol. 18, Issue.3,pp. 459-473,2106.

[10] Jelodar Hamed, and Javad Aramideh, "Presenting a pattern for detection of denial of service attacks with web mining technique and fuzzy logic approach", *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on*. IEEE, 2014.

[11] La Vinh Hoa, and Ana R. Cavalli, "A misbehavior node detection algorithm for 6LoWPAN Wireless Sensor Networks", *Distributed Computing Systems Workshops (ICDCSW), 2016 IEEE 36th International Conference on*. IEEE, 2016.

[12] Pongle Pavan, and Gurunath Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT", *Pervasive Computing (ICPC), 2015 International Conference on*. IEEE, 2015.

[13] Saghar Kashif, Mamoona Tariq, David Kendall,Ahmed Bouridane, "RAEED: A formally verified solution to resolve sinkhole attack in Wireless Sensor Network", *Applied Sciences and Technology (IBCAST), 2016 13th International Bhurban Conference on*. IEEE, 2016.

[14] Granjal Jorge, Edmundo Monteiro, and Jorge Sá Silva, "Security for the internet of things: a survey of existing protocols and open research issues",*IEEE Communications Surveys & Tutorials*, Vol.17, No.3,pp.1294-1312, 2015.

[15] Surendar M., and A. Umamakeswari, "InDReS: An Intrusion Detection and response system for Internet of Things with 6LoWPAN", *Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on*. IEEE, 2016.

[16] Tsitsiroudi Niki,Panagiotis Sarigiannidis, Eirini Karapistoli, "EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs", *Wireless and Mobile Networking Conference (WMNC), 2016 9th IFIP*. IEEE, 2016.

[17] Rahman Saoreen,Shamim Al Mamun, Mahtab Uddin Ahmed, M. Shamim Kaiser, "PHY/MAC layer attack detection system using neuro-fuzzy algorithm for IoT network", *Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on*. IEEE, 2016.

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

[19] Fang-jiao zhang, Li-dong zhai, Jin-cui yang and Xiang cui, “Sinkhole attack detection based on redundancy mechanism in wireless sensor networks”, Procedia Computer Science 31, Elsevier, pp.711-720, 2014.

[20] Kavita Tandon, “Sinkhole attack in wireless sensor network routing: A survey”, Research journal of computer and information technology sciences, vol.4, issue. 8, pp. 4-7, august 2016.

[21] Chaudhry Junaid Ahsenali, Usman Tariq, Mohammed Arif Amin, Robert G. Rittenhouse, "Dealing with sinkhole attacks in wireless sensor networks" Advanced Science and Technology Letters, vol. 29, issue. 2, pp. 7-12, 2013.

[22] Chakrabarty Shaibal, Monica John, and Daniel W. Engels, "Black routing and node obscuring in IoT." *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*. IEEE, 2016.

[23] Kumar Vijay, George Oikonomou, and Theo Tryfonas, "Traffic forensics for IPv6-based Wireless Sensor Networks and the Internet of Things", *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*. IEEE, 2016.

[24] Ibrahim Abdullah, Mohammad Muntasir Rahman, and Mukul Chandra Roy,"Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count", IJCNIS, vol.7, no.3, pp.50-56, 2015.DOI: 10.5815/ijcnis.2015.03.07

[25] *R. Stephen, A. Dalvin Vinoth Kumar, Dr. L. Arockiam, “*Deist: Dynamic Detection Of Sinkhole Attack For Internet Of Things”, *International Journal Of Engineering And Computer Science*, Volume 5, Issue 12, ISSN: 2319-7242, Page No. 19358-19362, Dec. 2016.