International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600

http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-231 PAGE NO: 1439-1444

Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

An Enhanced Sinkhole Attacker Node Identification Technique using Successful Link Ratio in IoT Environment

R. Stephen1, Dr. L.Arockiam2
Ph.D., Scholar**1,** Associate Professor2
Department of Computer Science,
St. Joseph's College (Autonomous), Tiruchirapalli, India.
Stephenr1989@gmail.com1, larockiam@yahoo.co.in2

***Abstract*—** The Internet of Things (IoT) is an emerging technology in the world. Devices are increasing day by day. So, people are connected with internet. IoT is sensor based technology. IoT has the role of sensing, processing and delivering of information. But, Internet of things is facing lots of issues and challenges. Particularly, security is one of the big challenges in internet of things environment. This paper deals with the security issues based on routing attacks in network. Routing attacks are the most destructive issue. The paper proposes watchdog technique to detect sinkhole attack in internet of things environment. The technique uses the successful link as parameter.

Keywords: IoT, Security, Routing, Sinkhole attack.

I. Introduction

The Internet of Things (IoT) provides a system for the monitoring and controling of the physical world through the collection, processing and analysis of generated data by IoT sensor devices. It is expected that by 2020 the number of connected devices will reach upto 50 billion. IoT devices are constrained devices due to limited power, storage, and memory capacity. IoT is used in different applications but the deployment of IoT applications is a challenge due to security problem. IoT security is a fundamental factor for secure communication among IoT sensor nodes. Particularly, secure routing for IoT sensor nodes need to be designed to provide a secure routing communication for IoT devices. The intruder takes advantage of the constrained devices to launch different routing attacks in IoT, such as selective forwarding, denial of service, sybil, wormhole attack and hello flood etc. Some existing approaches are proposed to detect and identify the routing attacks in IoT. These approaches are not given any sufficient solution for routing attacks.

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

II. Related Works

In related works, several papers proposed the different mechanisms for Internet of Things security. In which, 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.

III. Methodology

The proposed technique is used to identify the sink hole attacker node. Collection, processing, and validation are three phases used in proposed technique.

Collection phase: An important responsibility of this phase is to monitor routing node. This phase defines a monitoring module to count the transmission number of input and output performed by a node responsible for forwarding messages. Hence, the amount of incoming streams is equal to the number of output streams. If the amount of input and output streams is equal, the node is good. Otherwise, it’s assumed to have some deviations from the normal operation.

Processing phase: This processing phase is used to identify a sinkhole attack node. This module uses two kinds of evaluations. The evaluations are reputation and trust of a node. Reputation is the belief or perception of nodes to establish by iterations, actions or information exchange among them.

Validation phase: This phase uses the Beta Probability Density Function denoted by Beta (p\α,β). This function is used to estimate the state of each node behavior. Additionally, the beta (α,β) parameters are constantly updated.

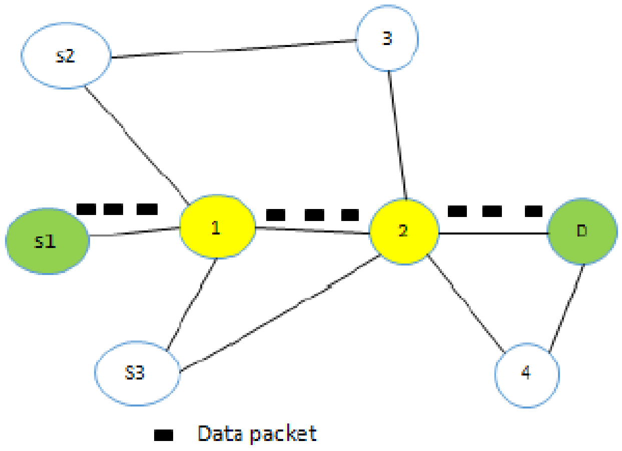

Fig 1. Successful Link based data packets transmission

Reactive protocol is active when the path is established by a node. Now, a source node sends the n number of data packets to destination node. In example scenario, source node (S1) sends the data packets to node1 (n1) at time (t1), source node S2 sends the data packets to node1 (n1) at time (t2) as shown in fig. 2 and source S3 sends the data packets to node (n1) at time (t3) as shown in fig. 3. Here, destination node (D) receives all the data packets from source node (S1). Here, S1 sends the data packets to node (n1) and n1 received the data packets and sends to node2 (n2). Finally, node2 (n2) sends all the data packets to destination node (D).

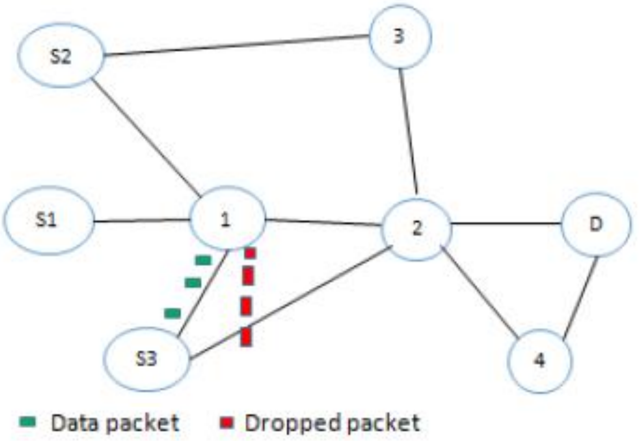

Fig 2. Failure link data packets dropped of source S3

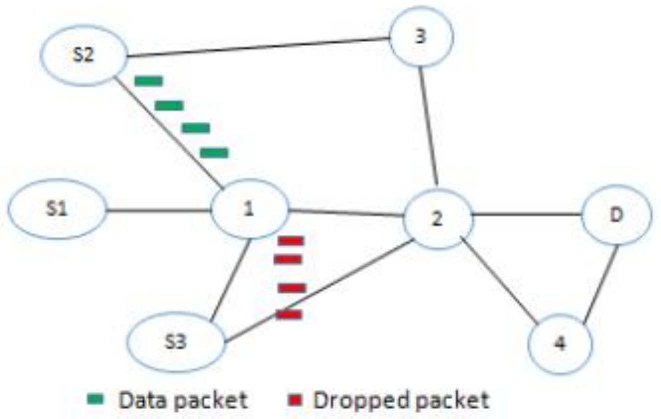

Fig 3. Failure link data packets dropped of source S2

The communication between source and destination nodes relays on the intermediate node 1. The watch dog technique is widely used to detect the sinkhole attacker node. The number of packets received and number of packets sent are the parameters used to identify the attacker node. When the ratio of number of packets sent, received are equal, then the node is reliable node.

The total number of packets is taken into consideration. The propose technique is used the number of successful links as the comparative parameter. The node1 successfully sent the packets sent by S1 but drops the packet from S2 and S3. S2 sends m number of packets and S3 sends k number of packets. So, the total number of packets sent to node 1 is (n + m + k) whereas the sent packets are only n numbers so dropped are (m + k).

When m + k is less than three by forth of n, then node1 is identified as trust node. In this case the proposed work identifies the total number of links. Existing system validates the node by number of sent packets. The fig. 4 shows one successful link and other two are failure. In the same figure, the next shows three successful links. The proposed work compares total number of successful links.

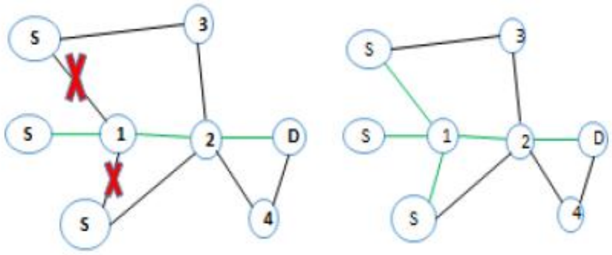

Fig 4. Successful link selection

IV. Conclusion

Many researchers proposed different techniques to detect sinkhole attack with successful received data packets as parameter. This paper used the number of successful link send the data packets to the destination as 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.

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.

[17] 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.

[18] 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.

[19] 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.