IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Novel Technique for Detection of Malicious nodes in IoT

Harsha Gupta[1*], Ekta Solanki[2], Anuj Kumar[3]

[1*,2,3]Dept. of Computer Science and Engineering, Institute of Technology and Management, AKTU, Lucknow, India

**Corresponding Author:harshaa.gupta1992@gmail.com, Mobile no: 8126656964*

Available online at: www.ijcseonline.org

Accepted: 18/Jul/2018, Published: 30/Jul/2018

Abstract: IoT is the technology in which the sensed information is aggregated to the base station, which is uploaded to the internet. Due to the decentralized nature of the network security, energy consumption is the major issue of the network. In the base paper technique, security to the network is provided in which uni-directional and bi-directional communication is possible. This research work is based on the misdirection attack on the network. The whole network is divided into fixed size clusters and cluster heads are selected in each cluster using LEACH protocol based on energy and distance. The technique of threshold-based is proposed in this work for the detection of malicious nodes from the network. The work is implemented using NS2.

Keywords: IoT, Ns2, Malicious Nodes, LEACH

I. INTRODUCTION

A worldwide system that connects all the computer networks with the help of a standardized Internet Protocol Suite (TCP/IP) to provide various services to them is known as the Internet. There are millions of users connected across the globe within the private or public sectors, business or government networks or within a local or a global range. The network interconnection of the regular objects is known as IoT. As there has been an increase in the growth of the speed of computations and networking, the IoT has led to a path of the smart universe [1]. IoT is a self-configuring type of network, which mainly interconnects all the things or objects present within the wireless network. Any item present within the real world that provides communication chain within the regions is known as an entity or object. The communication possibilities that can help in providing data transmission within certain paths with the help of various objects are the main goal of the IoT systems. On the basis of the properties like identification, confidentiality, integrity, as well as un-deniability, the security of data, as well as network, should be provided. Within various crucial areas related to the national economy, there are several IoT applications introduced apart from the internet. The applications such as medical service, health care as well as intelligent transportation are mostly found today. Thus, there is a need to provide higher availability as well as dependability within the IoT systems in order to provide efficient outcomes. The internet is extended to the physical world with the help of IoT technology due to which various security and privacy issues have risen [2]. The internal properties of IoT, as well as the differences of this technology against other traditional networks, are mainly the reasons for causing such issues. In order to attack the IoT systems, several adversaries have come up. The examination of various security issues as per the information flows and potential adversarial points of control is very important in order to protect the system from various attacks. There are various technologies used within IoT systems in order to ensure their security as well as privacy from various malicious users. A by-hop encryption technique is utilized within the traditional network layer in order to encrypt the information within the transmission process [3]. However, with the help of decryption and encryption operations, there is a need to keep plain text within each node. There is an end-to-end encryption mechanism applied within the traditional application layer. This means that for the sender as well as a receiver, the information is only kept explicit. There will always be encrypted information provided within the transmission process as well as during the forwarding of nodes. There are various solutions that ensure the integrity, authenticity, and confidentiality of communication due to the application of previously generated communication protocols. In order to encrypt the link present within the transport layer, the TLS/SSL is designed. Further, the network layer is protected through the designing of IPSec [4]. Thus, within each layer, integrity, authenticity, and confidentiality can be provided. There is a need to provide more privacy measures within the systems in order to secure the data. Nowadays, there are fewer numbers of communication security approaches also applied. There is frequently very less utilization of privacy measures even though lots of research has been done. There is a less frequent application of communication security mechanisms as well. As it is known that there is an increase in research by providing integrity and authenticity within the sensor data. Since the attacker can sense similar values when it places its own sensor physically closer to the sensor data, the confidentiality of sensor data is found less in demand [5]. There is a relatively less demand for confidentiality, thus within the sensor itself. Privacy is another major concern within these systems. In the physical world, the adoption of privacy measures is important in order to ensure the privacy of humans and objects. There are various internet security protocols that are utilized as per their properties within eh cryptographic algorithms. In order to encrypt data for confidentiality, the symmetric encryption algorithm is utilized usually. Advanced encryption standard (AES) block cipher is one of these symmetric encryption algorithms. Further, for the digital signatures and key transport, the asymmetric algorithms are utilized [6]. Rivest Shamir Adelman (RSA); the Diffie-Hellman (DH) asymmetric key agreement algorithm are two such algorithms. In order to ensure integrality, the SHA-1 and SHA-256 secure hash algorithms are used. In the security access protocol, the two types of communication are possible between the gateways and the mobile devices. The data from the mobile devices is transmitted to the gateway which is transmitted to the IP-based backbone. The IP-based backbone will transmit data to service platforms. The Diffie-Hellman algorithm is applied to establish a secure channel between the mobile devices and gateways for the bidirectional communication [7]. In the communication, the mobile device will select one public key and also select private key which is permitted root of a public key. The gateway will also select one public key and also make a private key which is a primitive root of a public key. The secure channel is established between both parties when they agreed on the common key “k”. The data from the mobile device will be transmitted to the gateway through the established secure channel.

II. LITERATURE REVIEW

P. Wortman et.al (2017) stated that the IoT devices are widely being used in the medical and healthcare domains. In this research, the issue of poor security designs and implementation in medical IoT devices was addressed by proposing the utilization of existing modeling software AADL (Architecture and Design Language) as a method of institutionalization of medical IoT device development [8]. Generally speaking, the method would eventually need to measure the performance of these large IoT networks, however, it is found that the result is totally different without some planning from a development stance. Consequently, this work proposed utilizing the powerful and flexible modeling language AADL to account for constraints and different concerns of over-engineering IoT devices inside the healthcare domain.

Z. Guo et.al (2016) proposed that the communication between the endpoints of devices with the help of physical objects present over the internet is known as the Internet of Things. There is a need of proper communication amongst the devices and humans in case of IoT systems for their proper usage. So, the biometrics provided a proper mechanism for convenience and security within the IoT applications [9]. The merits and demerits related to the biometric within the IoT systems are also described. There are various issues such as reverse engineering, tampering and unauthorized access within the IoT systems that are to be prevented with the help of various new biometrics merged within the previous ones. It is seen through the results achieved that the enhancement made has been beneficial.

T. Abels et.al (2017) research reviewed these with streamlining tradeoffs from a bottom-up approach utilizing DDS (Data Distribution Service). At that point, abnormal state semantic augmentations to DDS are suggested for semantics that was backward compatible while keeping up the security, reliability, and QoS of DDS [10]. At last, additional work is suggested toward out-of-the-box composability and interoperability between normal IoT information models and compliant arrangements. This author presents an SSN (Social Security Number) framework that consolidates the semantic endpoints of information-centric with strong semantics, supporting resource discovery for semantic sensor and event annotations. This initiates composable semantics, while extensions remained DDS compatible for proceeding with information security, QoS, and reliability.

M. Mohsin et.al (2016) proposed an ontology-based framework for the IoT for providing security to these systems. There are various APTs (Advanced Persistent Threats) that occur within the systems and can be prevented with the help of certain measures. The attack kill-chain is comprehended along with the leveraging of various attack examples and vulnerabilities. Further, the network semantics are aligned by providing appropriateness within the IoT systems [11]. There are various already existing ontologies within the CTI (Cyber Threat Intelligence) standards which needed to be examined here. The comparisons of these already stated mechanisms are done with the new concepts and the novel IoT ontology is proposed. From the XML-based threat feeds, the related information is extracted by the framework. The simulation results achieved here showed the improvements that have been mainly seen with the help of new changes made.

R. Kodali et.al (2016) presented that there were various remote interfacing and monitoring issues that aroused when a device was connected to the Internet in the case of IoT. This is done with the help of the Internet. The alarm is raised in an optional manner and the concerned systems are notified regarding this issue. This method could similarly be applied in the home automation systems with the help of various sets of sensors in the systems which notified the important things and helped the actions to be controlled as per required [12]. As per the experimental results, it could be seen that various enhancements when made within the systems, the applications could be made to run as per the needs of the users. Such enhancements are very useful and could be utilized in a huge number of applications mainly within the home automation systems.

III. RESEARCH METHODOLOGY

The whole network is deployed with the finite number of sensor nodes and the whole network is divided into fixed size clusters. The location-based clustering is applied to divide the whole network into the clusters. In each cluster, cluster heads are selected using the technique of LEACH Protocol. In the LEACH protocol, energy and distance of each node are checked, the node which has maximum energy and minimum distance from the other nodes is selected as the cluster head. All the nodes in the network will aggregate its data to its cluster head. The cluster head will establish a path through other cluster heads and transmit data to base station. To establish a path from source to destination, DSDV routing protocol is used. It maintains the information in the form of tables at every node. The source node selects the best path on the basis of hop count and sequence number. The path which has minimum hop count and maximum sequence number will be selected as the best path to the destination. The source nodes start transmitting data to the destination on the path. In the selected path, some malicious nodes are there which are responsible to trigger misdirection attack. To detect and isolate malicious nodes, the base station will apply the technique of node localization. In the technique of node localization, the base station will gather node information in terms of their location. The gathered information also contains the distance of each other from the base station. The distance factor leads to a counting delay on each hop which is on the established path. The base station when detecting that delay is increased on the established path. The base station starts counting delay on each hop, the node which increases the delay in the network so, it will be detected as the malicious node from the network.

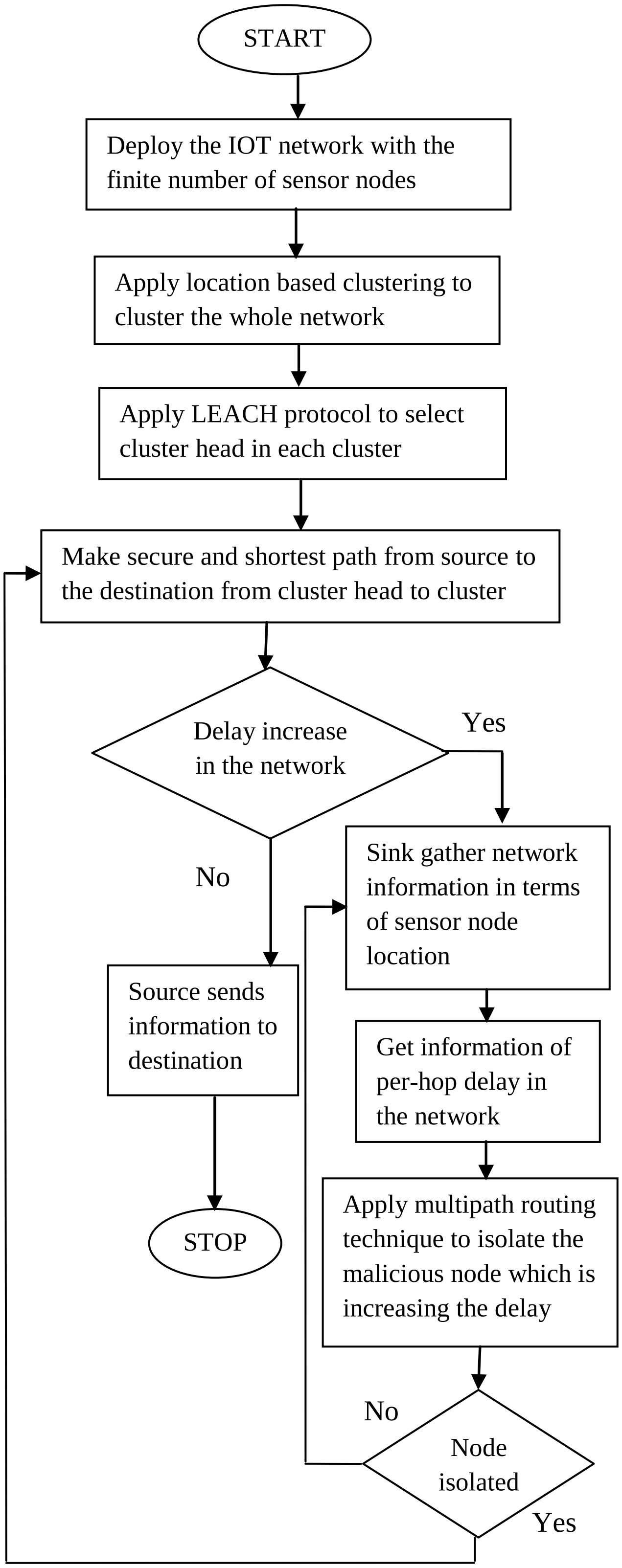
START
Deploy the IOT network with the finite number of sensor nodes
Apply location based clustering to cluster the whole network
Apply LEACH protocol to select cluster head in each cluster
Make secure and shortest path from source to the destination from cluster head to cluster
Delay increase in the network
Yes
No
Sink gather network information in terms of sensor node location
Source sends information to destination
Get information of per-hop delay in the network
Apply multipath routing technique to isolate the malicious node which is increasing the delay
STOP
No
Node isolated
Yes

Figure 1: Flowchart

IV. EXPERIMENTAL RESULTS

The proposed algorithm is implemented in NS2 and the results are evaluated by comparing the proposed and existing technique in terms of delay, energy, throughput, jitter, and packet loss. The results are shown below:

1. Delay:

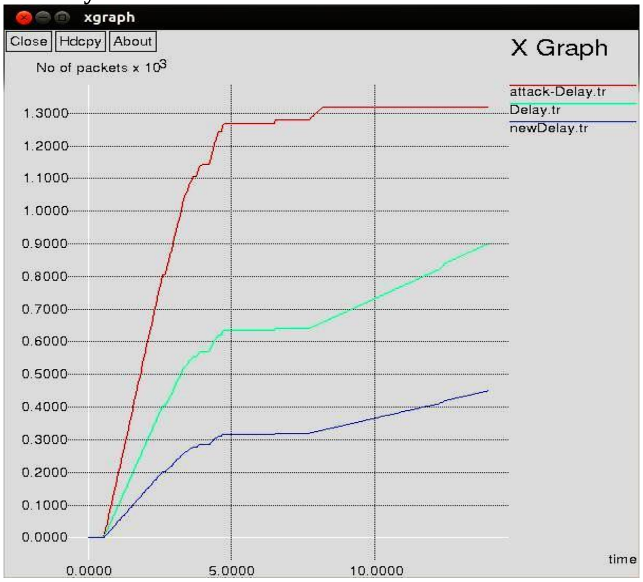

Figure 2: Delay graph

As illustrated in Figure 2, the Delay graph has been plotted. This graph shows the delay of without attack, with attack and the delay observed in the new proposed work. The performances are compared. It has been analyzed that delay in the attack scenario is maximum and delay is reduced in the proposed scenario due to the isolation of attack in the network.

2. Energy:

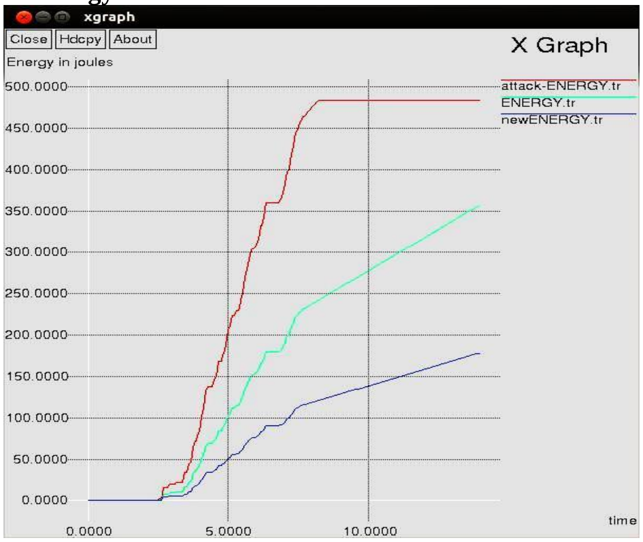

Figure 3: Energy graph

As illustrated in Figure 3, the energy consumption of the without attack, with attack and new proposed work is compared. Due to the attack on the network, the graph clearly shows that the energy consumption is more in the previous network. When the fault is removed from the network, energy consumption is reduced from the network.

3. Throughput:

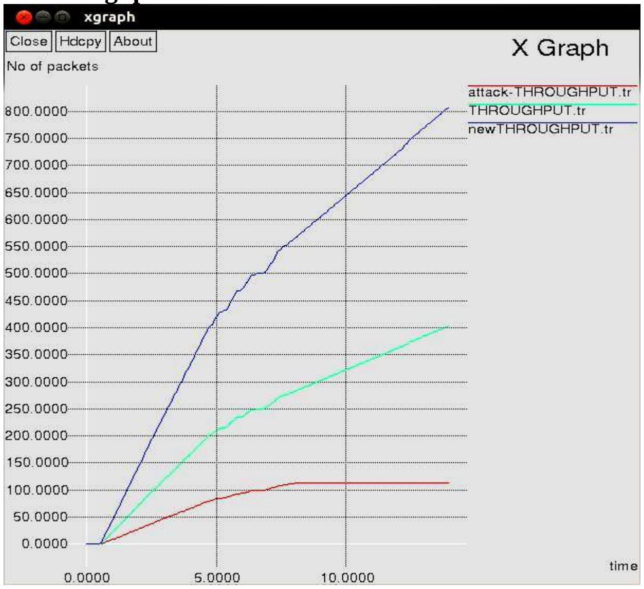

Figure 4: Throughput Graph

As shown in Figure 4, the comparison of without attack, with attack and the proposed scenario is shown in terms of throughput. It has been analyzed that throughput of the proposed scenario is maximum when the malicious node is isolated as compared to other two scenarios.

4. Jitter:

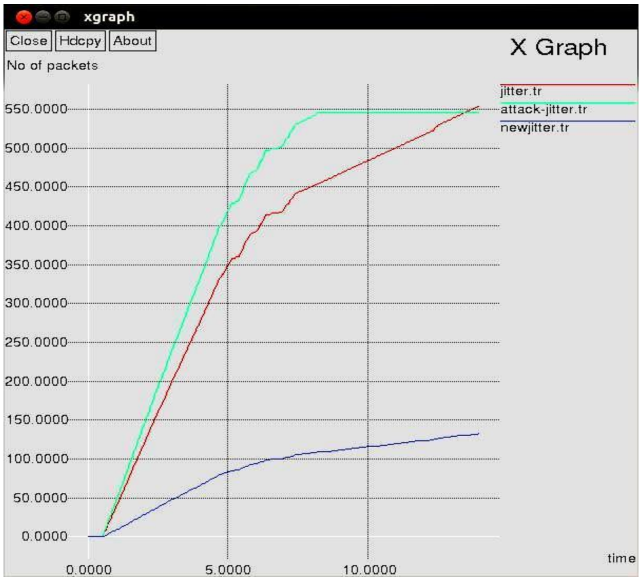

Figure 5: Jitter Graph

As shown in Figure 5, the comparison of without attack, with attack and the proposed scenario is shown in terms of jitter. It has been analyzed that jitter of the proposed scenario is minimum as compared to the other two scenarios.

5. Packet loss:

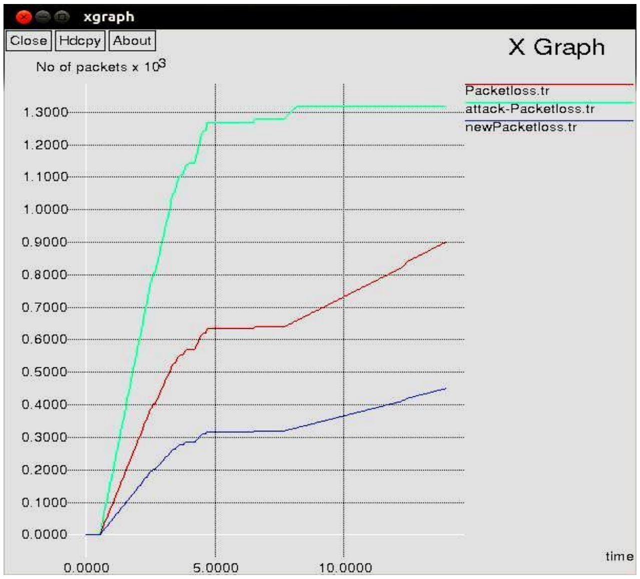

Figure 6: Packet Loss Graph

As shown in Figure 6, the comparison of without attack, with attack and the proposed scenario is shown in terms of packet loss. It has been analyzed that packet loss of the proposed scenario is minimum when the malicious node is isolated from the network as compared to the other two scenarios.

V. CONCLUSION

The internet of things is the technology which can sense information and pass it to the base station. The sensor nodes which are deployed in the network will sense information and pass it to the base station. The energy consumption and security are the various issues of this network. The security of the network gets compromised when the malicious nodes enter the network which triggers various type of active and passive attacks. The misdirection attack is the attack which reduces network performance in term of certain parameters. This research work is based on the detection and isolation of malicious nodes from the network which are responsible to trigger misdirection attack. The proposed technique is based on the threshold value, means the sensor node which is increasing delay than the threshold value is detected as a malicious node. The proposed and existing algorithms are implemented in NS2 and simulation results show that the proposed algorithm performs well in terms of certain parameters.

REFERENCES

[1] Z. Zhong, J. Peng, K. Huang, and Z. Zhong, “Analysis on Physical-Layer Security for Internet of Things in Ultra-Dense Heterogeneous Networks”, in Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 39-43, 2016.

[2] T. Charity, H. Hua, “Smart World of Internet of Things (IoT) and It's Security Concerns”, in Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 240-245, 2016.

[3] Mukhopadhyay, “PUFs as Promising Tools for Security in the Internet of Things”, IEEE Journal of Design and Test, vol. 33, no. 3, pp. 103-115, 2016.

[4] B. Sundaram, M. Ramnath, M. Prasanth, M. Sundaram, “Encryption and Hash-based Security in the Internet of Things”, in Proc. of IEEE International Conference on Signal Processing, Communication and Networking (ICSCN), vol. 3, pp. 1-5, 2015.

[5] V. Petrov, S. Edelev, M. Komar, and Y. Koucheryavy, “Towards the era of wireless keys: How the IoT can change authentication paradigm,” in IEEE World Forum on the Internet of Things (WF-IoT). Mar. 2014.

[6] A. Ranjan and G. Somani, “Access control and authentication in the internet of things environment,” in Computer Communications and Networks, pp. 283–305, 2016

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[8] P. Wortman, F. Tehranipoor, N. Karimian, and J. Chandy, “Proposing a Modeling Framework for Minimizing Security Vulnerabilities in IoT Systems in the Healthcare Domain”, in Proc. of IEEEEMBS International Conference on Biomedical & Health Informatics (BHI), pp. 185-188, 2017.

[9] Z. Guo, N. Karimian, M. Tehranipoor and D. Forte, “Hardware Security Meets Biometrics for the Age of IoT”, in Proc. of IEEE International Symposium on Circuits & Systems (ISCAS), pp. 1318-1321, 2016.

[10] T. Abels, R. Khanna, K. Midkiff, “Future Proof IoT: Composable Semantics, Security, QoS and Reliability”, in Proc. of IEEE Topical Conference on Wireless Sensor & Sensor Networks (WiSNet), pp. 1-4, 2017.

[11] M. Mohsin and Z. Anwar, “Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics”, in Proc. of International Conference on Frontiers of Information Technology (FIT), pp.23-28, 2016.

[12] R. Kodali, V. Jain, S. Bose and L. Boppana, “IoT Based Smart Security and Home Automation System”, in Proc. of IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1286-1289, 2016.