Chapter 48
Traffic Analysis Using IoT for Improving Secured Communication

K. Santhi Sri, P. Sandhya Krishna, V. Lakshman Narayana, and Reshmi Khadherbhi

Abstract Internet of Things can be simply referred to as Internet of entirety which is the network of things enclosed with software, sensors, electronics that allow them to gather and transmit the data. Because of the various and progressively malevolent assaults on PC systems and frameworks, current security apparatuses are frequently insufficient to determine the issues identified with illegitimate clients, unwavering quality, and to give vigorous system security. Late research has demonstrated that in spite of the fact that system security has built up, a significant worry about an expansion in illicit interruptions is as yet happening. Addressing security on every occasion or in every place is a really important and sensitive matter for many users, businesses, governments, and enterprises. In this research work, we are going to propose a secure IoT architecture for routing in a network. It mainly aims to locate the malicious users in IoT routing protocols. The proposed mechanism is compared with the state-of-the-art work and the results show that the proposed work performs well.

48.1 Introduction

Internet of Things can be simply referred to as Internet of entirety which is the network of things enclosed with software, sensors, electronics that allow them to gather and transmit the data. Smart homes and cities, connected cars, health care, smart farming, industrial Internet, manufacturing, smart retail are some of the applications of IoT [1]. There are many advantages of IoT: It provides more reliable communication and it is very efficient and saves time and money, increases business opportunities, increases

K. Santhi Sri (✉)
Department of Information Technology, Vignan's Foundation for Science, Technology & Research, Guntur, AP, India
e-mail: srisanthi@gmail.com

P. Sandhya Krishna · V. Lakshman Narayana · R. Khadherbhi
Department of Information Technology, Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur, AP 522009, India

A. N. R. Reddy et al. (eds.), *Intelligent Manufacturing and Energy Sustainability*,
Smart Innovation, Systems and Technologies 213,
https://doi.org/10.1007/978-981-33-4443-3_48

Fig. 48.1 Basic IoT architecture

productivity, and gives better quality of life. Not only advantages but there are some disadvantages in IoT: less privacy and low security, compatibility, and over-reliance on technology [2]. The major issue and challenge in IoT is security. Some of the security challenges in IoT are authentication, access control, confidentiality of data, trust, secure middleware, and privacy [3]. It is very important that the transmission of the data between IoT devices must be very secured [4]. The communication is possible by the routing protocols, and the data should be secured during the routing (Fig. 48.1).

Routing is a crucial factor in IoT which helps for communication between the devices and also transmission of data [5]. The execution of a good routing protocol can improve the performance of low power and lossy networks which are in short known as LLNs [6]. To evaluate the performance of a protocol, we can include the factors like energy utilization, control overhead, throughput, packet delivery ratio, and latency [7]. Routing is the main factor of complete IPV6 network for IoT. The routing protocols will make the IoT into reality [8].

In this research work, the idea is examining the security in routing protocols in IoT mainly in the network layer and the detailed description about the attacks on these routing protocols and some of their countermeasures and performance evaluation of these routing protocols when attack happens [9]. To address and route the data packets is the main goal of this layer. At this layer, using IP address the datagram from transport layer is enclosed to data packets, granted to their destinations [10, 11]. In this research work, Sect. 48.2 discusses the literature survey; Sect. 48.3 discusses the secure routing mechanism; Sect. 48.4 illustrates the experimental evaluation; and Sect. 48.5 concludes the research work.

48.2 Related Work

Montenegro et al. [1] proposed "Intrusion Detection System to Detect Sinkhole Attack on RPL Protocol in Internet of Things." IoT is primarily connected with wireless sensing networks and is subject to security problems like sinkhole attacks. The proposed IDS mechanism identifies such attacks on RPL and prompts the leaf nodes (sensor nodes) with a view to decrease the value of the packet loss. Here, the proposed mechanism calculates the intrusion ratio to identify the malicious nodes in the network.

Hui and Thubert [2] proposed "Review on Mechanisms for Detecting Sinkhole Attacks on RPLs." In this research work, major security challenges were centered around network layer and every method was examined and considered, and their uses and downsides and resource utilization are featured. At long last, a brief correlation was given, which demonstrates the historical organization of detecting methods for attacks like sinkhole, subsequently watching latest efficient technique.

Pongle and Chavan [5] proposed "Implementation of a Wormhole Attack Against a RPL Network: Challenges and Effects" and framed an attack in opposition to IEEE 802.15.4 WSAN by giving a wormhole execution. The proposed attack was applied to a genuine RPL topology. The analyses said the proposed attack can be compelling to undergo different attacks like a DoS. In the long run, we investigated the possibility of conceivable countermeasures.

Wallgren et al. [6] proposed "Performance Evaluation of RPL Protocol Under Mobile Sybil Attacks." Here, a trust-based IDS (T-IDS) solution was proposed in order to reduce sybil attacks under mobility in RPL. When RPL undergoes SybM, it is observed that the control overhead and the energy utilization were increased and the packet delivery ratio was decreased. The proposed T-IDS handles the issues that develop when RPL undergoes sybil attacks under mobility.

48.3 Proposed Work

Our structure expects that the client determines which router(s) fills in as the monitor(s); however, it is not clear how to pick the router(s) for this reason. In this part, we propose an approach to pick the area of the monitor(s) astutely so as to get a high precision rate. The terms DIO and DODAG refer to DODAG Information Object and Destination Oriented Directed Acyclic Graph, respectively.

Algorithm for Working of Router in RPL

Step 1: Receive a DIO (DODAG Information Object)
Step 2: Receive DIO the 1st time
If yes then follow the steps
Add the sender to the list of parent
Calculate the rank on the basis of objective function

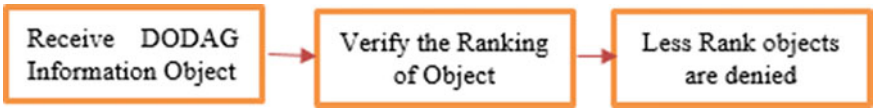

Fig. 48.2 Proposed model framework

Forward DIO's to others in multicast
If no then follow the steps
Satisfy criteria
If no
Then discard the packets
If yes
Then process the DIO
If rank not less than own_rank
Maintain the location in the DODAG
(Destination Oriented Directed Acyclic Graph)
Go to 3rd condition in step 2
If rank less than own_rank
Then improves the location and get lesser rank
The parents with the less rank will be denied
Go to 3rd condition in step 2

Step 3: End.

Another alternative is to utilize the proportion of between's centrality, which is a proportion of centrality in a chart dependent on most brief ways. The between's centrality of a hub v is given by the articulation $g(v) = \Sigma sf = vf = t\ \sigma st(v)\ \sigma st$, where σst is the complete number of most brief ways from hub s to hub t and $\sigma st(v)$ is the quantity of those ways that go through v. The proposed model framework is shown in Fig. 48.2.

Our flexible framework allows us to design another interesting strategy for choosing a router for the monitor. We train the detector on each one of the possible routers and estimate its performance [12]. We then select the router that achieves the highest accuracy rate to be the monitor.

Here, our proposed algorithm works mainly with two phases. In the first phase, we are going to identify the highest flow routers. Then, we can distribute the traffic based on other routes and based on selecting node for traffic diversion.

Identifying the attacker nodes (max flow nodes, traffic).
{
If (node)
Max traffic > threshold;
Place in a suspected list;
Evaluate the parents of those nodes;
If(node contains fake parents);
Take the id of the node and place them in a blocked list;

}

48.4 Experimental Results

The proposed method is implemented in ANACONDA SPYDER that performs traffic analysis for secure data communication [13]. The proposed method is compared with the traditional methods, and the results depict that the proposed method exhibits better performance than traditional methods.

1. **Throughput**

The rate at which packets were successfully delivered through a network channel is known as network throughput [14]. So, for the calculation of the value for the small networks, we can sum the packets received by all nodes. There are several ways to measure throughput (instantaneous or average) in a wired or wireless network using network simulators [15].

Formula
Throughput = sum (total count of true packets) * (average size of the packet))/total time sent to deliver that amount of data.

2. **Packet Delivery Ratio**

PDR is simply defined as the ratio between the packets that were generated by the source and the packets that were received by the destination.

Formula
Algebraically, it can be defined as:

$$\text{PDR} = N_1 \div N_2$$

where N_1 is the total sum of data packets which were received by the destination and N_2 is the total sum of data packets produced by the source.

3. **End-To-End Delay**

It is the difference between the time at which the sender generated the packet and the receiver received the packet. The end-to-end delay is also known as one-way delay which was being referred to time taken for the packet to transmit across the network from sender to receiver.

Formula
End-to-End Delay = Sum of (Delay at sender + Delay at receiver + Delay at intermediate nodes).

The proposed method monitors every node and checks for attackers based on their behavior, whereas the existing method does not monitor every node for secure data

communication. The throughput of the proposed method is high when compared to the traditional methods as the malicious users are effectively identified.

Here, Fig. 48.2 represents the throughput comparison between regular RPL protocol, existing secure RPL, and our proposed mechanism. Here, we simulate regular RPL protocol with different number of nodes varying from 100 to 500 without any attacker nodes. Existing and proposed mechanisms contain 5, 10, 20, 22, and 25 attacker nodes in each case. And we observe the performance, which is shown in Fig. 48.2. Here, regular RPL protocol has highest throughput compared to existing and proposed, but proposed is very near to standard RPL and more dominating than existing work.

Here, Fig. 48.3 represents the end-to-end delay comparison between regular RPL protocol, existing secure RPL [16], and our proposed mechanism. Here, we simulate regular RPL protocol with different number of nodes varying from 100 to 500 without any attacker nodes. And existing and proposed mechanisms contain 5, 10, 20, 22, and 25 attacker nodes in each case. And we observe the performance, which is shown in Fig. 48.2. Here, regular RPL protocol has very slight delay compared to existing and proposed, but proposed is closer delay to standard RPL and more dominating than existing work.

Here, Fig. 48.4 represents the packet delivery ratio comparison between regular RPL protocol, existing secure RPL, and our proposed mechanism. Here, we simulate regular RPL protocol with different number of nodes varying from 100 to 500 without any attacker nodes. And existing and proposed mechanisms contain 5, 10, 20, 22, and 25 attacker nodes in each case. And we observe the performance, which is shown in Fig. 48.2. Here, regular RPL protocol has highest delivery compared to existing

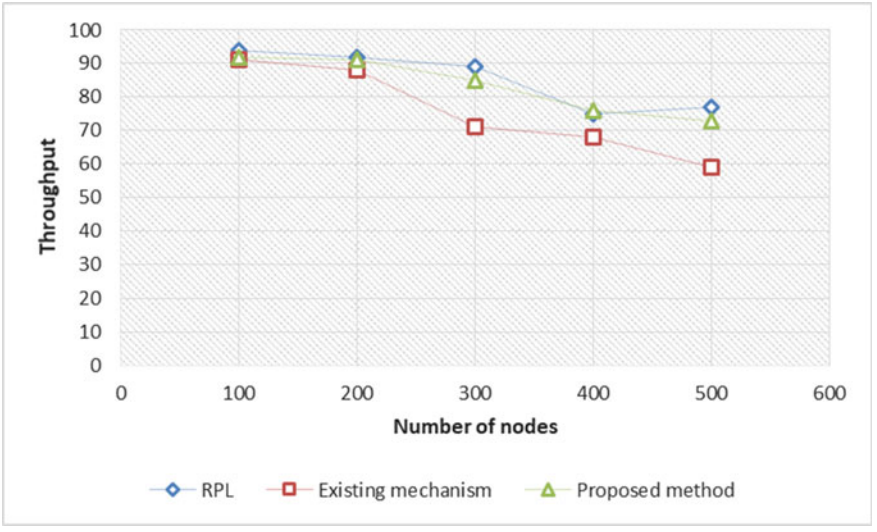

Fig. 48.3 Throughput

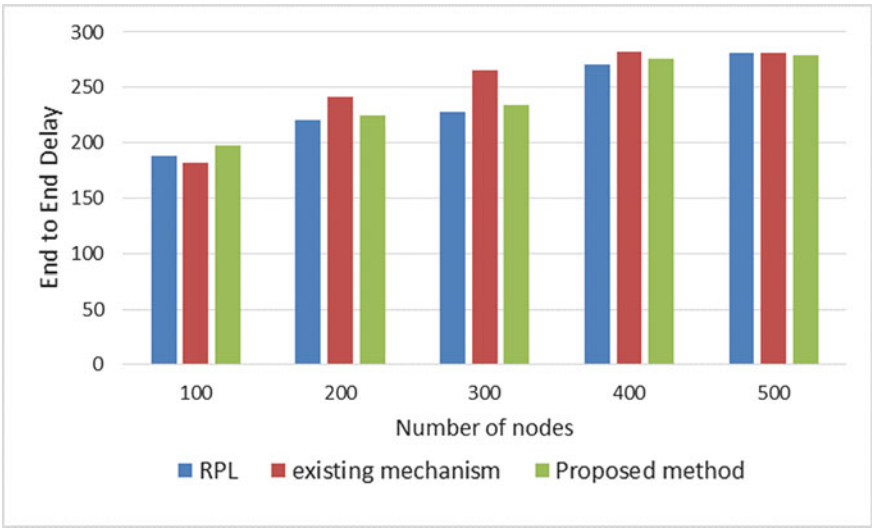

Fig. 48.4 E2E delay

and proposed, but proposed is very near to standard RPL and more dominating than existing work (Fig. 48.5).

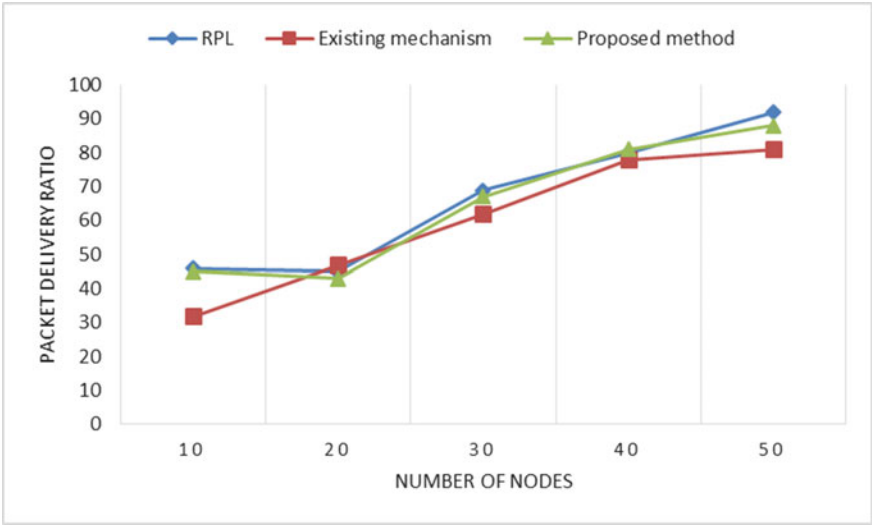

Fig. 48.5 Packet delivery ratio

48.5 Conclusion

Secure communication is a prime thing in any kind of network. IoT is a very huge network and in order to make secure communication is a very difficult thing. Many routing protocols are proposed in IoT for routing. But most of them are suffering from secure communication. This research work mainly focuses on secure communication between different IoT nodes, for that we use a monitor-based mechanism in a network, identify the malicious nodes, and made the communication secure. The proposed mechanism performs well when compared to literature mechanisms. In the future, the security of the devices can be improved by allotting an authority to monitor during data transmission.

References

1. G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, Transmission of IPv6 packets over IEEE 802.15.4 networks, in *IETF RFC 4944*, Sept. 2007. https://tools.ietf.org/html/rfc4944
2. J. Hui, P. Thubert, Compression format for IPv6 datagrams over IEEE 802.15.4-based networks, in *IETF RFC 6262*, Sept 2011. https://tools.ietf.org/html/rfc6282.
3. H. Tschofenig, T. Fossati, Transport layer security (TLS)/datagram transport layer security (DTLS) profiles for the Internet of Things, in *IETF RFC 7925*, July 2016. https://tools.ietf.org/html/rfc7925
4. E. Kim, D. Kaspar, J. Vasseur, Design and application spaces for IPv6 over low-power wireless personal area networks (6LoWPANs), in *IETF RFC 6568*, Apr. 2012. https://www.ietf.org/rfc/rfc6568.txt
5. P. Pongle, G. Chavan, A survey: attacks RPL and 6LowPAN in IoT, in *International Conference on Pervasive Computing (ICPC 2015)*, Pune, India (2015), pp. 1–6
6. L. Wallgren, S. Raza, T. Voigt, Routing attacks and countermeasures in the RPL based internet of things. Int. J. Distrib. Sens. Netw. **9**(8), 1–11 (2013)
7. TCG, Guidance for securing IoT using TCG technology, Sept. 2015. https://www.trustedcomputinggroup.org/guidancesecuring-iot-using-tcg-technology-reference-document
8. A. Roger, T. Tsao, V. Daza, A. Lozano, M. Richardson, M. Dohler,A security threat analysis for the routing protocol for low-power and lossy networks (RPLs), in *IETF RFC 7416*, Jan. 2015. https://tools.ietf.org/html/rfc7416
9. H. Baba, Y. Ishida, T. Amatsu, K. Maeda, Problems in and among industries for the prompt realization of IoT and safety considerations, *IETF Draft*, Oct. 2016. https://datatracker.ietf.org/doc/draft-baba-iot-problems
10. M.A. Iqbal, M. Bayoumi, Secure end-to-end key establishment protocol for resource-constrained healthcare sensors in the context of IoT, in *International Conference on High Performance Computing & Simulation (HPCS)* (2016), pp. 523–530
11. J.L. Hernandez-Ramos, J.B. Bernabe, A. Skarmeta, ARMY: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things. IEEE Commun. Mag. **54**(9), 28–35 (2016)
12. D. Hardt, The OAuth 2.0 authorization framework, in *IETF RFC 6749*, Oct. 2012. https://www.ietf.org/rfc/rfc6749.txt
13. S. Gerdes, L. Seitz, S. Gerdes, G. Selander, An architecture for authorization in constrained environments, in *IETF Draft*, Aug. 2016. https://www.ietf.org/id/draft-ietf-ace-actors-04.txt
14. O. Garcia-Morchon, S. Kumar, M. Sethi, Security considerations in the IP-based Internet of Things, in *IETF Draft*, Feb. 2017, Available: https://www.ietf.org/id/draft-irtf-t2trg-iot-seccons-01.txt.

15. K. Moore, R. Barnes, H. Tschofenig, Best current practices for securing Internet of Things (IoT) devices, in *IETF Draft*, Oct. 2016. https://tools.ietf.org/html/draft-moore-iot-security-bcp-00.
16. V.H. La, R. Fuentes, A.R. Cavalli,A novel monitoring solution for 6LoWPAN-based wireless sensor networks,in *22nd Asia-Pacific Conference on Communications (APCC)* (2016), pp. 230–237