International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Trust Based Technique for the Mitigation of Version Number Attack in Internet of Things

Chandni, Rakesh Kumar

Abstract*: The internet of things is the self-configuring type of network in which sensor nodes join or leave the network. The version number is the active type of attack possible in DODAG protocol of IoT. The Shield technique is proposed in the previous research work for the mitigation of version number attack in the network. It is very much complex for the detection of malicious nodes. In this research work, the trust based mechanism is proposed for the isolation of version number attack. The trust based mechanism calculates trust of each sensor node. The sensor nodes with the least trust are identified from the network as malicious nodes. The proposed mechanism is implemented in network simulator version 2. The trust based mechanism and shied based techniques are implemented and results are analyzed in terms of throughput, delay, control message overhead and average power consumption. It is analyzed that in terms of all parameters trust mechanism performs well as compared to shield based technique.

Keywords: Shield Technique, Trust Technique, Version Number Attack

I. INTRODUCTION

The Internet of Things is the network form of self-configuration and decentralization. Because of this type, malicious nodes join the network that causes different kinds of active and passive attacks of Things is the self-configuring and decentralized type of network. Because of this type, malicious nodes join the network that causes different kinds of active and passive attacks [1]. Depending upon the link amongst objects, the objects function autonomously. Analysis of collected data to make decisions, providing lightweight data and extracting the data by accessing and authorizing the cloud-based resources are some of the actions performed by IoT nodes [2]. The users, services, sensors as well as objects are linked to each other very closely through IoT, which are deployed in the apps ranging from smart grid healthcare apps to smart transport technologies. The number of smart devices and intelligent services provided through IoT networks has been outgrowing due to the huge business opportunities provided in the IoT scenarios [3]. The cloud-based IoT networks have been developed due to the relativity of IoT devices on the cloud infrastructure such that the data can be transmitted across applications [4]. There are mainly IP based web and IoT applications which provide transmission using TCP and UDP. However, among most of the IoT applications, there are few commonly used message distribution functions. Various applications implement these functions in interoperable standard ways [5]. Very similar to the client/server protocol, a publish/subscribe protocol. architecture is designed which is called MQTT (Message Queue Telemetry Transport). Due to its simple structure and ability to avoid high CPU and memory utilization, MQTT protocol is known to be of huge important. Another protocol that is designed from the financial industry is the Advanced Message Queuing Protocol (AMQP) [6]. The TLS/SSL protocols are used here to manage the security. To ensure that less power and memory embedded devices are being used, CoAP is applied for communication. Various network layer protocols also have been designed. The most commonly known IoT standard for MAC is the IEEE 802.15.4 [7]. A frame format is defined in this protocol in which the source and destination addresses are defined in headers along with the manner in which nodes can communicate. Low power multi-hop networking is applied lately in IoT because it is not suitable to use frame formats applied previously in traditional networks since they cause overhead in these systems [8]. For ensuring high reliability, less cost and meeting the communication requirements of IoT, channel hoping and time synchronization are used. Destination Oriented Directed Acyclic Graph (DODAG) is a category of Directed Acyclic Graph that is rooted in the sink and utilizes RPL routing protocol to organize routers. [9]. The DODAG Information Object (DIO) messages originate from the DODAG root periodically to initiate DODAG formation. The link-local multicast is used to advertise this generated DODAG [10]. Information related to the root identity of DODAG, the used routing metrics, and the depth/ rank of originating router are included within the DIO messages [11]. The router that joins the DODAG describes its own rank, depending on the data advertised by its neighbors within their DIO's. For ensuring that the global repair process of RPL is under control and all the nodes available in DODAG are updated as per the routing state, the root node uses version number [12]. The lifetime of IoT system is reduced due to the presence of version number attacks in it. Attacker can perform this attack with very less expense and the network can be overloaded by exploiting the global repair mechanism that is included as an immune system of protocol.

Manuscript published on 30 September 2019
* Correspondence Author
Chandni*, Computer Science & Engineering, National Institute of Technical Teachers Training & Research, Chandigarh, India.
Rakesh Kumar, Computer Science & Engineering, National Institute of Technical Teachers Training & Research, Chandigarh, India

With the presence of several inconsistencies in the network, a global repair is initiated by the root [13]. DODAG's version number is increased to rebuild the entire DODAG. DODAG Information Object (DIO) is the control message that contains this version number.

Comparisons are provided between the current version number and the one that each receiving node receives from its parent [14]. In case of higher received version, the current rank information is ignored, the trickle timers are reset and a new procedure for joining the DODAG is initiated. In this global repair, a loop-free topology is ensured, although its cost is very high. It can be known that the node did not migrate to the new DODAG version if the previous value of version is being advertised in DIO messages [15]. The other nodes must not select such a node as preferred parent. Two versions of DODAG may occur at the moment of global repair. However, data packets that exist in old version can transit in new version for avoiding loops [16]. The previous version is not considered as DODAG and there is no guarantee of availability of loop free topologies as the network is still beyond convergence state.

II. Literature Review

Ahmet Aris et al. [17], suggested the removal of RPL version number attacks by two easy alleviation methods. The updates of the version number from the way of leaf nodes were eliminated by the first mitigation approach. The first approach gave information about the toughness of the locations for virtual numbers. The first mitigation approach was not useful for mitigating the invasion from the other invasion locations. The second mitigation technique was capable of mitigating the effect of the attack without considering the locations of the attack. In the second approach, the nodes could change their virtual number only when the mass number of closest nodes having better ranks claimed updated virtual number. The efficiency of the proposed approach was verified by using a number of topologies. In future, more experiments can be performed in the area of various virtual number invasions situation. The examination of the hybrid mitigation approach can also be performed in the near future.

Amit Dvir et al. [18] suggested using a new routing protocol to eliminate the Low Power and Lossy networks problems. This protocol was named as IPv6 routing protocol. The main objective of this routing protocol was to grant the functionality in the Low power and Lossy Networks. By constructing and managing the directed acyclic graphs through one or more gateway, the RPL provided pathway multiplicity. An updated version named DODAG was used for reconstructing the routing topology. It was also suggested that for the prevention of initial intruder, same approach should be used, for publishing the decreasing value of rank. In this method, a wider part of the DODAG was combined with the DODAG through the intruder for forwarding a long part of the network traffic. Thus with the use of this new security component, the illegal increase in the version number could be avoided.

Anthea Mayzaud et al. [19], presented a novel classification approach for the categorization of the attacks found besides the RPL. For this approach, mainly three classes of attacks were considered. The lifespan of the network was reduced by the invasions against resources. The intruder node capture and the examined a wide part of the network in case of attacks. The researchers have proposed a lot of approaches for the prevention of these types of attacks based on different properties. The implementation and the management of the security modes were not mentioned by the RPL specification technique. Thus it was concluded that the transaction among different security levels was a major challenge for the accepted structure of RPL networks.

H. Abdo et al. [20], proposed a novel approach for ensuring the security and safety in case of industrial threat investigation. For this purpose, a conventionally used safety investigating system named bowtie analysis was combined with the newly developed version of security analysis. The modified version was named as attack tree analysis. A comprehensive demonstration of the risk scenario was presented by the combination of attack tree and bowtie analysis approach in terms of safety and security. For the evaluation of risk range relied on two term similar parts, a new mechanism was presented. The one part was for security while the other part was for safety. The tested results showed that the proposed approach performed well. In future, a more reliable and tough likelihood estimation technique will be developed by the researchers.

Ahmet Aris et al. [21], presented a deep study of RPL version number attacks. The investigation of the attacks was also performed which was based on different scenarios. The investigation was performed on a practical network topology containing both mobile and stationary nodes. These nodes contained a number of cardinalities. The research work was based on IETF routing requirements. A probabilistic approach was used for calculating the attacks probabilities. The performance results were demonstrated according to the different valves of p. The outcomes of the simulation depicted that the mobile attackers and the distantly placed nodes had almost same effects on the network performance. In future, a study about the coming behavior of DIO information for the recognition of possible position of virtual number attack will be performed.

Hezam Akram Abdul-Ghani et al. [22], proposed a new internet of things suggestion approach relied upon constructing blocks policy. This was basically a four layered reference model. An inclusive IT invasion model was developed including four main phases. Firstly an IoT asset relied invasion plane comprising of four mechanism was presented. These components were software, information, protocol wrapping the entire IoT stack and substantial objects. In the second phase, a pattern of IoT security aim was defined. The IoT invasion classification for every component was identified in the third phase. In the final phase, violation of security aims and the association among every attack was identified. A set of solution was also for protecting each asset was also identified in the last phase also. For the very first time, an IoT invasion model relied on building block reference model was developed.

III. RESEARCH METHODOLOGY

A. Trust Based Technique

A trust management protocol based on a social trust in a community-based social IoT environment and update trust value using both direct observations and indirect recommendations.

$$T_{ij}^{x}(t) = (1-\alpha)T_{ij}^{x}(t-\Delta t) + \alpha T_{ij}^{x,direct}(t), if\ j == k;$$

X = community-interest, cooperativeness and honesty.

- **Direct trust observations**

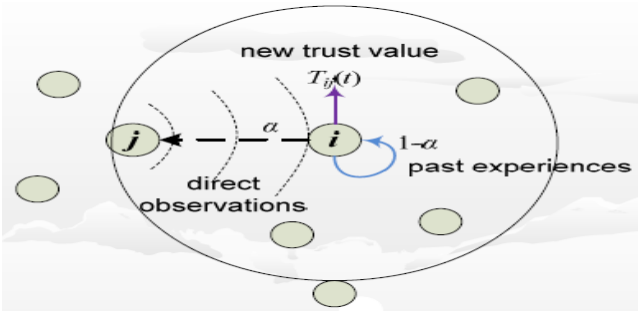

Fig.1. Direct Observation Trust.

$T_{ij}^{honesty,direct}$ refers to honesty value based on the direct observation of node j to i. $Tijcooperativeness,direct$ gives the degree of cooperativeness of node j to I based on direct observations over range of [0, t]. The figure 1 indicates the process of how node I evaluates node j with direct observation and past experiences.

- **Indirect recommendations**

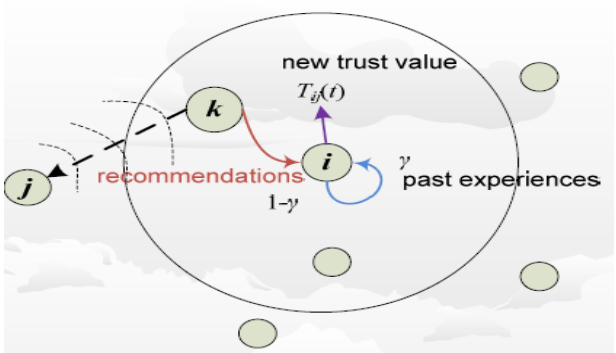

Fig. 2. Indirect recommendations.

$$\Gamma = \frac{\beta T_{ik}^{X}(t)}{1+\beta T_{ik}^{X}(t)}, T_{ij}^{X}(t)(1-\gamma)T_{kj}^{X}(t-\Delta t) + \gamma T_{kj}^{X,recom}(t)$$
$$if\ j! = k;$$

In this equation, T_{ij}^{X} provides the trust value of recommendation of node k towards node i. The contribution of recommended trust mechanism increases with proportionally as either T_{ij}^{X} or β increases. The figure 2 indicates the process of how node i evaluates node j with recommendation and past experience.

B. Proposed Algorithm

Input: Sensor Nodes
Output: Detection of Malicious nodes
Step 1. Deploy the network with limited amount of sensor nodes.
Step 2. Divide the entire network into clusters of fixed size.
Step 3. Choose the cluster head based on range and energy consumption in each cluster.
Step 4. Calculate Trust
  Step 4.1. Check number of packets transmitted by the sensor node.
    Step 4.1.1 Number of packets forwarded is calculated by equation below.

$$P(forward_q|delivered) = \frac{p(delivered|forward_q)(p(forward_q)}{\sum_{m-1}^{n}\binom{n}{m}p^{m}_{delivered}{}^{(1-p_{delivered})^{n-m}}}$$

    Step 4.1.2. The PDR is calculated by the equation given below.

$$PDR = \frac{p(delivered|forward_q)(p(forward_q)}{\sum_{m-1}^{n}\binom{n}{m}p^{m}_{delivered}{}^{(1-p_{delivered})^{n-m}}} \cdot \frac{1}{P_{TPF}}$$

    Step 4.1.3. PDR define that total number of packets forwarded in the network by the source node
Step 5. If (PDR < Threshold PDR)
  Step 5.1. Mark Sensor node as malicious
Step 6. Establish new path from source to destination
Step 7. Transmit data throughput newly selected path
End.

C. Performance Analysis Parameters

Throughput: - The throughput is the parameter which is used for the performance analysis. It measures the number of packets received successfully in the per unit time at the destination.

Packet Delivery Ratio:- The packet delivery ratio is the parameter that measures the amount of packets sent by source node and the amount of packets received by destination.

Delay: - A network's delay indicates how long it takes to move from one node or endpoint to another for a bit of information across the network.

$$Delay = Time\ received - Time\ sent.$$

Control Message Overhead: It's an indirect computing time consisting of memory, bandwidth, or other resources to perform a particular task.

$$Control\ Message\ Overhead = Total\ packets\ sent - data\ packets$$

Average Power Comparison: -It is used to predict the lifetime of wireless sensor network, thus each sensor node is depended on battery node.

*Power Consumption = No. of packets*per unit energy*

IV. RESULTS AND DISCUSSION

In order to address the challenges and achieve efficiently, we need to test and improve the research algorithms before they are exposed to the reality. In the field of IoT research, establishing a network of IoT in the real scene is very difficult, a single test bed takes up a lot of time and costs. Fortunately, with the help of simulation tools, we can easily get the analysis, monitor the process and evaluate the security and safety of a trust model. Researchers could easily deploy, layout and configure the nodes through writing scripts. However, different simulation tools have different properties. In this research work NS2 is used as a simulator to test the reliability of the technique.

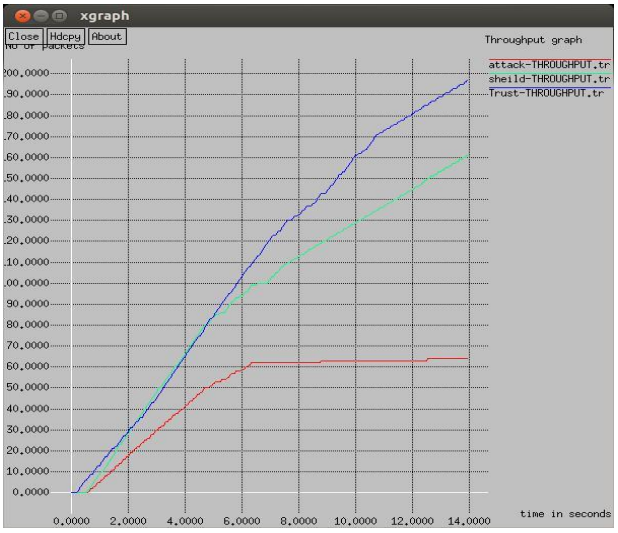

Fig. 3. Throughput Comparisons.

As shown in figure 3, the performance assessment compares the efficiency of the proposed and existing algorithm.It is analyzed the throughput of the proposed algorithm is high as compared to existing algorithms.

Table-I:Throughput Analysis

Simulation Time	Attack Scenario	Sheild Technique	Trust Based Technique
2 seconds	19 packets	30 packets	30 packets
4 seconds	40 packets	68 packets	68 packets
10 seconds	61 packets	130 packets	160 packets
14 seconds	63 packets	160 packets	190 packets

In table I, it is analyzed that proposed scenario has maximum throughput as compared to other two shield and attack scenario.Due to detection of malicious nodes present in the network the attack scenario has maximum loss of packets and more collisions occur in the network,which causes less amount of packet to reach at destination and thus minimum throughput.

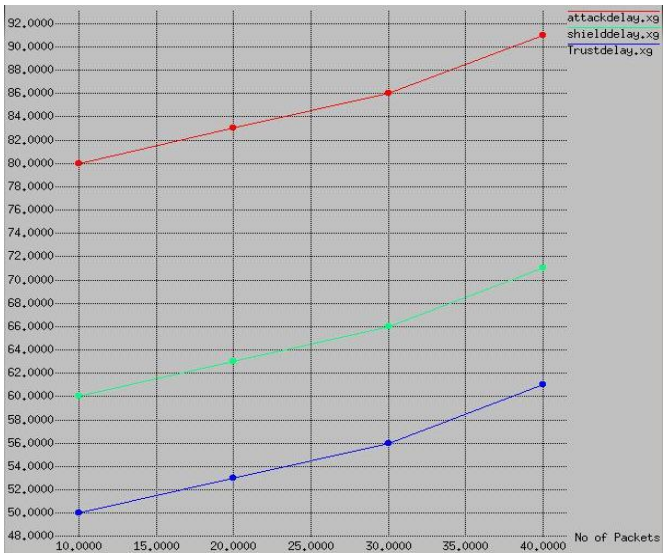

Fig. 4.Delay Comparison.

As shown in figure 4, a network's delay indicates how long it takes for a set of data to move from one node or endpoint to another. The red line in the graph shows the attack scenario where maximum number of packets are dropped and delay for every packet is more as compared to shield and trust based technique.

Table -II: Delay Analysis

No. of Packets	Attack Scenario	Sheild Technique	Trust Based Technique
10 Packets	80 millisecond	60 millisecond	50 millisecond
20 Packets	83 millisecond	63 millisecond	53 millisecond
30 Packets	86 millisecond	66 millisecond	56 millisecond
40 Packets	91 millisecond	71 millisecond	61 millisecond

The value obtained for each time slot with Attack, Shield and trust based techniques for delay, is shown in the table II.In case of attack scenario there was no security and malicious nodes in the network causes the packet to drop,or to hold the packet for longer period of time ,which causes the un-neccesary retransmissions in the network, and delay to increase but in case of proposed technique more relaible path is selected to transmit the packets.

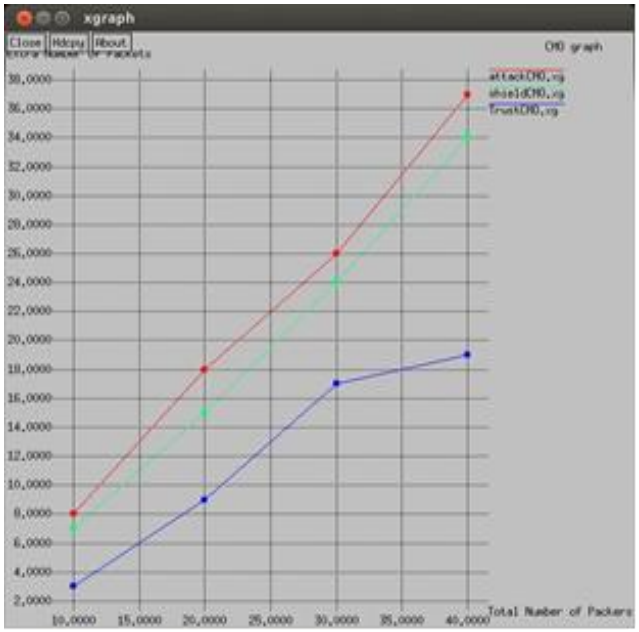

Fig. 5. Control Message Overhead Comparison.

As shown in figure 5, Control Message Overhead is time to perform a particular job of indirect computation consisting of memory, bandwidth, or other resources. Three scenarios are compared which are attack scenario, shield attack and trust based technique. Shield scenario is evaluated as the method used to isolate the attack of version number. The proposed scenario is the method based on trust to isolate version number attack. Compared to other techniques, the proposed scenario has less overhead control message for isolating the version number attack in the network.

Table-III: Control Message Overhead Analysis

No. of Packets	Attack Scenario	Sheild Technique	Trust Based Technique
10 packets	8	7	3
20 packets	18	15	9
30 packets	26	24	17
40 packets	37	34	19

The values obtained for Control Message Overhead in each Scenario for the different number of packets is shown in the table III.

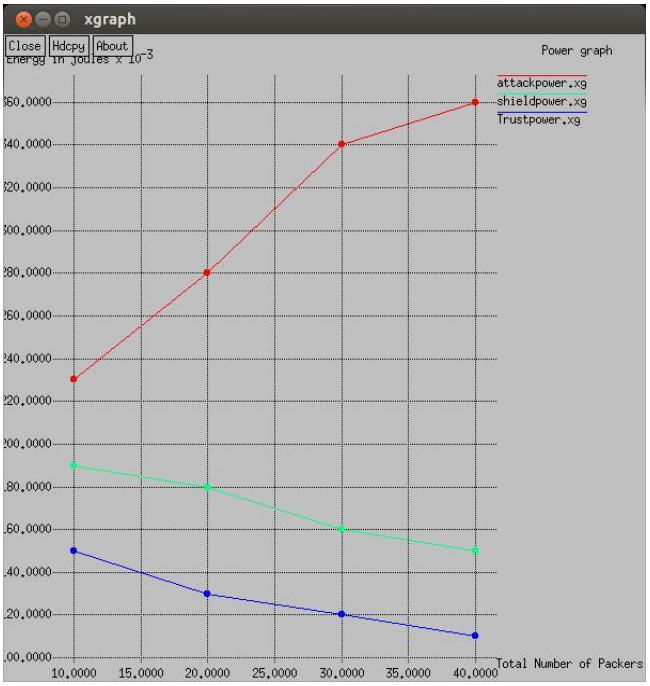

Fig. 6. Average Power Consumption.

As shown in figure 6, Wireless sensor network life is predicted, as each sensor node depends on the battery node.The proposed scenario has least average power consumption as compared to other technique for the isolation of VNA in the network.

Table-IV: Control Message Overhead Analysis

No. of Packets	Attack Scenario	Sheild Technique	Trust Based Technique
10 packets	0.23joules	0.19 joules	0.15 joules
20 packets	0.28 joules	0.18 joules	0.13 joules
30 packets	0.34 joules	0.16 joules	0.12 joules
40 packets	0.36 joules	0.15 joules	0.11 joules

The values obtained for the Average Power Consumption in each Scenario is shown in the table IV.

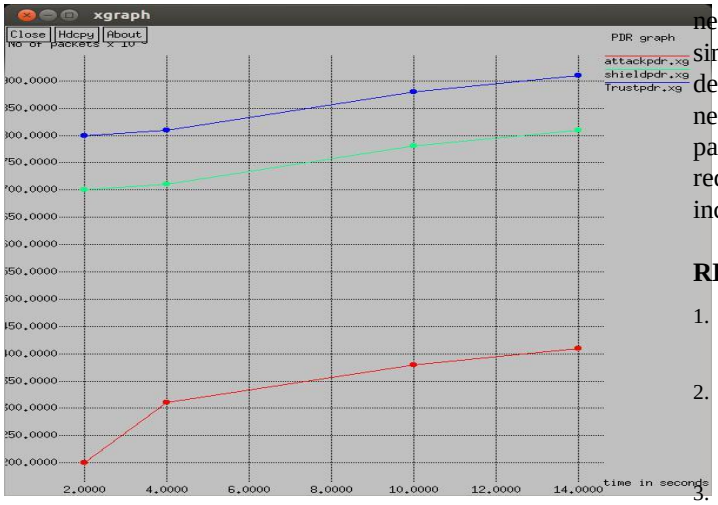

Fig.7. Packet Delivery Ratio.

Packet delivery calculation relies on the data packet transmitted and generated, In case when there is congestion in the network and there is decent traffic supervision, data packets may well train up at the source and does not come in the network on any occasion. Individual packets will never make any contribution to throughput, but never effect the Packet Delivery Ratio as these packets were never sent over the network. As shown in figure 7, Red line indicates the attack scenario when the packet delivery ratio for transmission of packets is less and as the proposed technique is applied based on the calculation of trust values, the best possible path is selected to transmit the packet which has less number of loop generated in the network.

Table-V: PDR Analysis

Simulation Time	Attack Scenario	Sheild Technique	Trust Based Technique
2 seconds	200 packets	700 packets	800 packets
4 seconds	301 packets	701 packets	801 packets
10 seconds	380 packets	708 packets	888 packets
14 seconds	401 packets	801 packets	901 packets

Table V shows the PDR values obtained in different techniques with respect to simulation time and it can be seen that the trust based technique has maximum PDR value.

V. CONCLUSION

This research work is related to mitigating the version number attack in Internet of Things (IoT). The DODAG is a hierarchical topology which is used in RPL for small devices in which the malicious nodes increases the version number, Due to which the path that contains loop get created in the network. The trust based mechanism is proposed in this research work for mitigating version number attack from the network, and will detect the malicious nodes. The trust based mechanism will consume least number of resources from the network. Therefore proposed scenario is applied in network simulator version 2 and results are analyzed in terms packet delivery ratio, control message overhead, throughput and network delay. It is analyzed that after the proposed scenario packet loss and power consumption and network delay reduces whereas throughput and packet delivery ratio increases while comparing to other two scenarios.

REFERENCES

1. D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wirel. Pers. Commun.*, vol. 58, no. 1, pp. 49–69, 2011.
2. V. Bhuvaneswari and R. Porkodi, "The internet of things (IoT) applications and communication enabling technology standards: An overview," *Proc. - 2014 Int. Conf. Intell. Comput. Appl. ICICA 2014*, pp. 324–329, 2014.
3. E. Hopalı and Ö. Vayvay, "Internet of Things (IoT) and its Challenges for Usability in Developing Countries," vol. 2, no. January, pp. 6–9, 2018.
4. H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, pp. 648–651, 2012.
5. E. Baccelli, M. Philipp, and M. Goyal, "The P2P-RPL Routing Protocol for Ipv6 Sensor Networks: Testbed Experiments," *SoftCOM 2011, 19th Int. Conf. Software, Telecommun. Comput. Networks, Split*, vol. 1, pp. 1–6, 2011.
6. T. Zhang and X. Li, "Evaluating and analyzing the performance of RPL in contiki," *Proc. first Int. Work. Mob. sensing, Comput. Commun. - MSCC '14*, pp. 19–24, 2014.
7. J. Posegga, T. Eder, D. Nachtmann, D. Parra, and D. Schreckling, "Conference Seminar SS2013 — Real Life Security (5827HS) Trust and Reputation in the Internet of Things Trust and Reputation in the Internet of Things," pp. 1–19, 2013.
8. Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, "A Trust-based Resilient Routing Mechanism for the Internet of Things," *Proc. 12th Int. Conf. Availability, Reliab. Secur. - ARES '17*, pp. 1–6,
9. A. Mayzaud, R. Badonnel, and I. Chrisment, "A distributed monitoring strategy for detecting version number attacks in RPL-based networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 14, no. 2, pp. 472–486, 2017.
10. J. Guo, I. R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in internet of things systems," *Comput. Commun.*, vol. 97, pp. 1–14, 2017.
11. S. N. M. García, J. L. Hernández-Ramos, and A. F. Skarmeta, "Test-based risk assessment and security certification proposal for the Internet of Things," *IEEE World Forum Internet Things, WF-IoT 2018 - Proc.*, vol. 2018–Janua, pp. 641–646, 2018.
12. J. Guo and I. R. Chen, "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems," *Proc. - 2015 IEEE Int. Conf. Serv. Comput. SCC 2015*, pp. 324–331, 2015.
13. I. R. Chen, F. Bao, and J. Guo, "Trust-Based Service Management for Social Internet of Things Systems," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 6, pp. 684–696, 2016.
14. M. A. Joanna Głowacka, Jarosław Krygier, "A Trust-Based Situation Awareness System for Military Applications of the Internet of Things," *J. Sound Vib.*, vol. 189, no. 2, pp. 161–171, 2015.
15. M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, 2014.
16. B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, 2017.
17. A. Arış, S. B. Örs Yalçın, and S. F. Oktuğ, "New lightweight mitigation techniques for RPL version number attacks," *Ad Hoc Networks*, vol. 85, pp. 81–91, 2019.
18. A. Dvir, T. Holczer, and L. Buttyan, "VeRA - Version number and rank authentication in RPL," *Proc. - 8th IEEE Int. Conf. Mob. Ad-hoc Sens. Syst. MASS 2011*, pp. 709–714, 2011.
19. A. Mayzaud, R. Badonnel, and I. Chrisment, "Detecting version number attacks in RPL-based networks using a distributed monitoring architecture," *2016 12th Int. Conf. Netw. Serv. Manag. CNSM 2016 Work. 3rd Int. Work. Manag. SDN NFV, ManSDN/NFV 2016, Int. Work. Green ICT Smart Networking, GISN 2016*, pp. 127–135, 2017.

20. H. Abdo, M. Kaouk, J. M. Flaus, and F. Masse, "A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis," *Comput. Secur.*, vol. 72, pp. 175–195, 2018.
21. A. Aris, S. F. Oktug, and S. Berna Ors Yalcin, "RPL version number attacks: In-depth study," *Proc. NOMS 2016 - 2016 IEEE/IFIP Netw. Oper. Manag. Symp.*, no. Noms, pp. 776–779, 2016.
22. H. Akram, D. Konstantas, and M. Mahyoub, "A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, 2018.

AUTHORS PROFILE

Chandni received her Bachelor of Technology in Computer Science and Engineering from Guru Nanak Dev University, Gurudaspur. At present, she is pursuing Master of Technology in Computer Science and Engineering from National Institute of Technical Teacher Training and Research, Chandigarh. Her key area of interest includes Algorithms, Internet of Things and Networking.

Dr. Rakesh Kumar received his Bachelor of Technology in Computer Science and Engineering from Punjab Technical University, Jalandhar, India in 2004. Master of Technology in Information Technology from Guru Gobind Singh Indraprastha University, New Delhi, India in 2008. Ph.D in Computer Engineering from National Institute of Technology Kurukshetra, India in 2015. At present, he is working as an Assistant Professor in the Department of Computer Science and Engineering at the NITTTR. His research interests includes Discrete Mathematics, Cloud computing, Data Mining, Software Testing with special focus on Mobile Adhoc Networks and Wireless Sensor Networks.