IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Simulation analysis of Denial of Service attack over scalable IoT networks

Author

**Professor, CSE Department, M. M. Engineering College, M. M. University, Ambala, India

ABSTRACT-. Using Internet of Things (IoT) communication between different types of devices networks is promising but it may arise various security issues as IoT offers data exchange over an open platform. In this paper, various threats over IoT will be explored and a security solution against denial of service (DoS) attack will be presented for reliable and secure communication over IoT. Its performance will also be measured using various parameters (Throughput/Routing Load/Packet Delivery Ratio/Energy Consumption).

Keywords- IoT, smart devices, DoS, Security, Intrusion

I. INTRODUCTION

Capabilities of existing networks can be extended by using Internet of Things (IoT) and it offer following applications in different domains as given below:

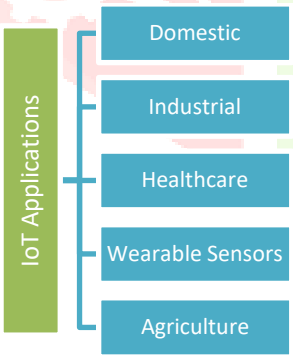

Figure:1 IoT applications

Figure:1 shows different IoT based applications as discussed below:

(i) Domestic: It offers interactive home appliances, energy management, surveillance solutions for home usage.

(ii) Industrial: It supports robotics and automation, quality control and maintenance etc.

(iii) Healthcare: It deals with patient's data collection, monitoring and analysis that can be used for decision making and diagnosis.

(Iv)Wearable Sensors: Users can wear sensors to record statistics of entire body and maintain healthy lifestyle.

(v) Agriculture: It offer crop monitoring, drone based pest control and environmental data collection etc.

IoT operates over heterogeneous environment that consists of different types of devices (mobile/sensors) and applications those can interact with each other using internet in an open environment thus may cause security concerns as discussed follows:

- **Authentication and Data privacy:** IoT enable devices may access the network resources anytime and there is need to verify the authenticity of each device but in case of a large IoT network, it may be a complex operation.
- **Intrusion detection:** Intrusion over network resources may occur as IoT devices exchange data using open network environment.
- **Trust management and access control:** For data exchange in a secure environment, there is need to restrict the access over network resources as well as there is another major issues related to trust management between neighbors due to scalable network [1] [2][3].

In IoT, each layer has different types of security concerns as discussed below:

(i) Perception Layer: It consists of physical and MAC layer and deals with the field data collection and may have following threat types:

- **Tampering:** Intruder can physical damage the field sensors to interrupt transmission.
- **Impersonation:** Intruder can reproduce the identity of malicious nodes as legitimate nodes.

(ii) Application layer: It manages end user data and can have following security concerns:

- **Denial of services:** It can interrupt the transmission for end user and network will be no longer accessible.
- **Fabrication:** Transmitted data can be overwritten by intruder.
- Integrity: Data can be updated at intermediate transmission stage and user will get altered data.
- **Confidentiality:** Data can be tracked or analyzed by unauthorized users.

(iii) Network layer: It ensures the access to network resources and it can be compromised by following attacks:

- **Transmission interception:** Transmission can be jammed using jammers.

- **Routing attack:** Intermediate routing paths can be intercepted to redirect routing [4] [5][6].

Researchers addressed above security issues and investigated various solutions as discussed in next section.

II. Literature Survey

A. R. Rao et al. [6] investigated the various security concerns intrusion/authentication/authorization/privacy) over IoT platform and found that block chain based security provision can be used to encounter these issues on the cost of extra resource consumption.

E. H. Abualsauod [7] proposed a solution for IoT-UAV network. It uses a hybrid blockchain algorithm to secure the communication over network. Analysis shows that it has optimal resource consumption/ delay and computational time.
A. Dan Potorac et al. [8] investigated the cyber security concerns associated with IoT network and study found that data fabrication, privacy and unauthorized access are few common issues those can be resolved by implementing a standard security provision.

D. T. Do et al. [9] investigated the security issues of physical layer in IoT network and implemented an intelligent surface between IoT devices and intermediate access points to measure signal to noise ratio that may vary during security attack. Analytical study shows that it can guard the network against eavesdropping successfully as well as offers low computational cost.

M. A. Jan et al. [10] studied the security threats related to data privacy/authentication over multimedia IoT network in healthcare domain. Analysis found that blockchain based security provision is more reliable as compared to traditional cryptography methods.

A. Raghuvanshi et al. [11] investigated the behavior of heterogeneous devices under security threats and analysis specifies that identification of devices is a major concern during data exchange over IoT network due to lack of standard authentication provision.

L. Logrippo et al. [12] presented a rule based security provision to secure IoT network. It subdivides the devise by assigning labels and enforces access control list to secure network resources. Analysis shows that IoT offer robust security/privacy and data integrity but it is performance affected by application compatibility level.

R. Ur Rasool et al. [13] investigated the impact of intelligent boat tools that can trigger the attack against IoT based healthcare services and it is difficult to trace them. Study found that traditional security provisions cannot detect such types of threats and machine learning algorithms can be utilized to trace boat attacks.

A. Raghuvanshi et al. [14] investigated the security threats over various layers IoT networks. Analysis found that each layer has different threat type. At application layer, it is difficult to ensure the device identity, data privacy whereas network layer suffers from man denial of services attack and physical layer can be compromised replay attack.

R. Faqihi et al. [15] highlighted the common security associated with IoT network in social domain. It found various concerns related to compatibility of security provision with applications, large key size, threat detection accuracy, computational overhead lack of standard security policy etc.

Y. Zhang et al. [16] introduced an energy efficient solution to secure IoT network. It secures the sampling using a Chaotic encryption method followed by arnold transformation and solo assessment diffusion. Results indicates its outcomes in terms of low computational cost w.r.t. resource consumption.

B.K. Mohanta et al. [17] explored the various security threats over IoT network and examined the role of machine learning methods for these threats. Survey shows that machine learning can be used to develop a trust model, threat analysis can also be performed as well as services like authentication/ authorization/traffic analysis etc.

O. P. Singh et al. [18] presented a solution to secure IoT based health care services. It uses a watermarking over data to retain its privacy. Analysis shows it performance in terms of optimal resource consumption.

R. Yu et al. [19] developed a method to analyze traffic patterns (incoming and outgoing) over IoT using domestic applications. Analysis shows that it can accurately analyze the different traffic types (i.e. HTTP and TCP) to trace various threats (denial of services/malware/memory overflow/injections).

I. Sadek et al. [20] developed a method that provides end to end secure communication for IoT based healthcare services. Analysis shows that it can efficiently guard the network against intrusion but secure transmission between gateways and field sensors is still an open issue.

III. Simulation Analysis of DoS Attack under IoT Node's Density

Denial of Services (DoS) atatck is a serious threat for IoT communication and in this paper, a simulation based analysis is conducted under various constrains i.e. variations in node's density and intruder's density.
Network simulator (NS-3) was used for simulations over IoT platform with different parameters i.e. node's density varies from 10-100, intruder's density varies from 0-5 (0 means there is no intruder), Rx/Tx 25, terrain 1800*1800, initial energy 15J etc. and performance is analyzed as per following parameters:

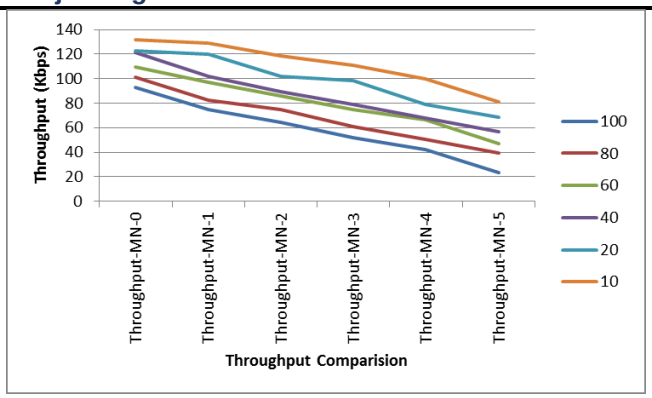

Figure: Throughput- Comparison -Node-10-100

Figure: shows the comparison of Throughput w.r.t. IoT-Node density that varies from 10-100 under the constraints of malicious nodes that vary from 0-5. Results indicate that if there is no malicious node, network delivered throughput between 131.5555556Kbps to 93Kbps using 10 to 100 IoT nodes. With only one malicious node, it varies 129.2222222 kbps to 75Kbps, with 2 malicious nodes, it varies from 118.3333333Kbps to 64Kbps, with 3 malicious nodes, it varies from 110.6666667Kbps to 51.88888889Kbps, with 4 malicious nodes, it varies from 99.66666667Kbps to 42.33333333Kbps and with 5 malicious nodes, it is 80.77777778Kbps to 23.11111111Kbps w.r.t. node density.

Figure: shows the comparison of packet delivery ratio (PDR) w.r.t. IoT-Node density that varies from 10-100 under the constraints of malicious nodes that vary from 0-5. Results indicate that if there is no malicious node, network delivered PDR between 93.00864 to 65.7502 using 10 to 100 IoT nodes. With only one malicious node, it varies 91.3589945 to 53.02435192, with 2 malicious nodes, it varies from 83.66064415 to 45.24744698, with 3 malicious nodes, it varies from 78.24037706 to 36.68499607, with 4 malicious nodes, it varies from 70.46347211 to 29.92930086 and with 5 malicious nodes, it is 57.10919089 to 16.33935585 w.r.t. node density.

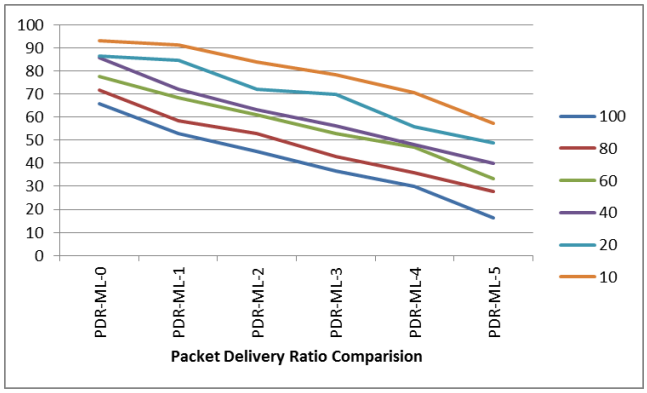

Figure: PDR- Comparison -Node-10-100

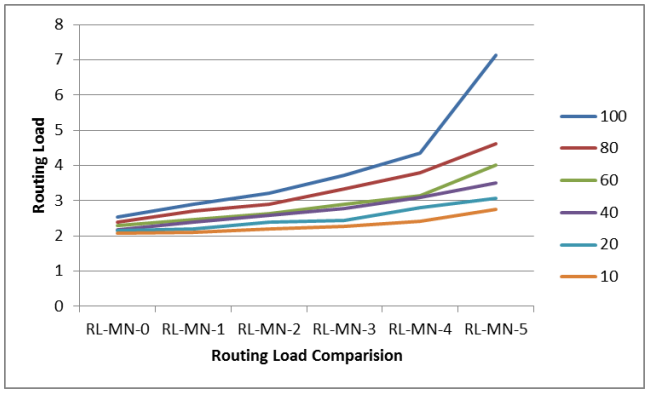

Figure: Routing Load- Comparison -Node-10-100

Figure: shows the comparison of routing load w.r.t. IoT-Node density that varies from 10-100 under the constraints of malicious nodes that vary from 0-5. Results indicate that if there is no malicious node, is is between 2.075169 to 2.520908 using 10 to 100 IoT nodes. With only one malicious node, it varies 2.094582975 to 2.885925926, with 2 malicious nodes, it varies from 2.195305164 to 3.210069444, with 3 malicious nodes, it varies from 2.27811245 to 3.725910064 , with 4 malicious nodes, it varies from 2.419175028 to 4.341207349 and with 5 malicious nodes, it is 2.751031637 to 7.120192308 w.r.t. node density.

IV. CONCLUSION

In this paper, impact of intruder density 0-5 over IoT network under the constraints of DoS attack has been analyzed by varying IoT-node density 10-100. Simulation results illustrate that if number of intruder varies then the performance parameters also varies and it is inversely proportional to the intruder's density. If there is no DoS attack, network delivered highest Throughput/PDR with minimal routing load. However Throughput/PDR slightly degraded due to IoT-nodes's density. In case of medium node density 40-60, routing load increases and rest of all parameters are declined. In case of highest node density 80-100, its performance is degraded.

In case of single intruder, DoS attack has minimal affect over the network performance and there are marginal changes in performance parameters. In case of intruder density 2-4, there is sharp decline in network performance and in case of maximum intruder density 5 with highest IoT node density, network could not delivered the acceptable outcomes.

As per the above discussion, it can be concluded that there are two different constraints (density of IoT Node/ intruder density) that act as barrier for the performance of IoT network because as the node density increased, routing load is also increased thus reduced t eh overall performance. Similar to that, w.r.t. node density, if there is variation in intruder's density over legitimate node' density thus further degrades the performance.

In future, a solution will be developed to secure routing against DoS attack over IoT networks under the scalable and mobile network environment.

V. REFERENCES

[1] J. Neeli, S. Patil,"Insight to security paradigm" , research trend & statistics in internet of things(IoT), Global Transitions Proceedings,Vol.2 (1), Elsevier-2021,pp.84-90.

[2] N. Tariq, F. A. Khan, M. Asim, "Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis", Procedia Computer Science, Vol.191, Elsevier-2021,pp.425-430.

[3] J. R. Uribe, E. P. Guillen, L. S. Cardoso, "A technical review of wireless security for the internet of things: Software defined radio perspective", Journal of King Saud University - Computer and Information Sciences, Vol.34, (7),Elsevier-2022,pp.4122-4134.

[4] S. Chaudhary, R. Johari, R. Bhatia, K. Gupta A. Bhatnagar, "CRAIoT: Concept, Review and Application(s) of IoT" 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE-2019, pp.1-4.

[5] G. Shi, H. Hao, J. Lei and Y. Zhu, "Application security system design of Internet of Things based on blockchain technology", International Conference on Computer, Internet of Things and Control Engineering (CITCE), IEEE-2021, pp. 134-137.

[6] A. R. Rao, D. Clarke,"Perspectives on emerging directions in using IoT devices in blockchain applications", Internet of Things, Vol. 10, Elsevier-2020,pp.1-16.

[7] E. H. Abualsauod, “A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network, “Computers and Electrical Engineering, Vol.99,Elsevier-2022,pp.1-20.

[8] A. Dan Potorac, "Vulnerabilities and new critical security challenges of the Internet of Things (IoT)", Biomedical Engineering Applications for People with Disabilities and the Elderly in the COVID-19 Pandemic and Beyond, Academic Press,Elsevier-2022, pp.325-333.

[9] D. T. Do, A.T. Le, N. Duy X. Ha, N. N. Dao, "Physical layer security for Internet of Things via reconfigurable intelligent surface", Future Generation Computer Systems, Vol. 126,Elsevier-2022, pp. 330-339.

[10] M. A. Jan, J. Cai, X. C. Gao, F. Khan, S. Mastorakis, M. Usman, M. Alazab, Paul Watters, "Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions", Journal of Network and Computer Applications, Vol.175,Elsevier-2021,pp.1-77.

[11] A. Raghuvanshi, U. K. Singh, M. Shuaib, S. Alam, “An investigation of various applications and related security challenges of Internet of things”, Materials Today: Proceedings, Elsevier-2021,pp.1-4.

[12] L. Logrippo, "Multi-level models for data security in networks and in the Internet of things", Journal of Information Security and Applications,Vol.58, 2021,pp.1-13.

[13] R. Ur Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, J. Qadir, "Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML", Journal of Network and Computer Applications, Vol. 201,Elsevier-2022, pp.1-15.

[14] A. Raghuvanshi, U. K. Singh, "Internet of Things for smart cities- security issues and challenges", Materials Today: Proceedings, Elsevier-2020,pp.1-3.

[15] R. Faqihi, J. Ramakrishnan, D. Mavaluru, "An evolutionary study on the threats, trust, security, and challenges in SIoT (social internet of things)", Materials Today: Proceedings, Elsevier-2020, pp.1-8.

[16] Y. Zhang, Y. Xiang, L.Y. Zhang, "Internet of Things Security. In: Secure Compressive Sensing in Multimedia Data", Cloud Computing and IoT. SpringerBriefs in Electrical and Computer Engineering, Springer-2019, pp.83–112.

[17] B.K. Mohanta, D. Jena, "Internet of Things Security Using Machine Learning. In: Patnaik, "Advances in Machine Learning and Computational Intelligence", Algorithms for Intelligent Systems. Springer-2021, pp.129-136.

[18] O. P. Singh, A. Anand, A. K. Agrawal, A. K. Singh, "Electronic Health Data Security in the Internet of Things through Watermarking: An Introduction," Internet of Things Magazine, Vol.5 (2), IEEE-2022, pp.55-58.

[19] R. Yu, X. Zhang and M. Zhang, "Smart Home Security Analysis System Based on The Internet of Things," 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), 2021, pp. 596-599.

[20] I. Sadek, J. Codjo, S. Ul Rehman, B. Abdulrazak, "Security and privacy in the internet of things healthcare systems: Toward a robust solution in real-life deployment", Computer Methods and Programs in Biomedicine Update, Vol.2,Elsevier-2022,pp.1-8.