Detection of VN Attack in Iot Using Trust-Based Technique

Shivam Sharma[1], Dr. Anita Ganpati[2]
[1]Dept of Computer Science
[2]Professor, Dept of Computer Science
[1, 2] Himachal Pradesh University, Shimla, India

Abstract- *The Internet of Things, or IoT, is a recent advancement in Computer Science and Information Technology which makes it possible for Smart Devices to connect wirelessly to the network. The phrase, which combines the concepts internet and things, uses both terms separately. Using the aforementioned technology, items such as mobile smartphones, Smart TVs, Air Conditioners, etc. are connected to one another. In this paper, a finite number of sensor nodes are deployed in the simulated environment. The Version Number Attack is then triggered into the simulated environment which is based on the RPL routing Protocol.*

The above work is based on Destination Oriented Directed Acyclic Graph is a kind of Directed Acyclic Graph which is rooted at the source and employs RPL routing protocol to arrange the routers (DODAG). In this paper, a finite number of sensor nodes are triggered into the simulation network. In earlier research, the Shield Approach was put forth as a means of reducing version number attacks on network. It is quite difficult to identify faulty nodes. It is recommended to use the trust-based technique to isolate version number attacks. Each sensor node's trust is calculated using the trust-based process. The internet identifies the sensors that have the lowest level of trust as compromised nodes. In a previous study, the shield technique as well as trust-based mechanisms were used, and the results were assessed in aspects of throughput, delay, CMO, and average power consumption. In this study, however, only three metrics Packet Loss, Latency, and Control Message Overhead are used to evaluate performance, using 38 sensor nodes in a virtual environment where a version number attack is triggered. The three parameters have an overall analysis that can be used to assist and therefore draw conclusions about the work performedin this study. Analysis shows that the Proposed Technique outperforms the Existing Technique and Attack Scenario, in the other two aspects.

Keywords- IoT, RPL, DODAG, Delay, Latency.

I. INTRODUCTION

The Internet of Things, or IoT, is a new technology in the field of CS&IT in which smart gadgets are connected to the internet through wireless means. Radio Frequency Identification (RFID) and Sensor Network Technologies are rising to meet this new challenge of invisibly embedded information andcommunication systems in the environment. The term "Internet of Things" is combined from two words: the first one is "Internet," and the second one is "Things." The Internet is a global network of interconnected computer networks that uses the standard Internet protocol suite (TCP/IP) to provide service to billions of people around the globe [1]. The Internet of Things (IoT) has become a hot topic of discussion both inside and outside the business due to a massive increase in the number of objects connected to the internet by wire or wireless [2]. The Internet of Things is expected to transcend all previous industrial revolutions, surpassing technological marvels such as the steam locomotive, printing press, and electricity. The fourth industrial revolution is marked by the "Internet of Things," as well as robots, machine learning, nanotechnology, computing, biotechnology, 3D printing, and autonomous vehicles [3]. Destination Oriented Directed Acyclic Graph is a kind of Directed Acyclic Graph which is rooted at the source and employs RPL routing protocol to arrange the routers (DODAG). The DODAG root regularly generates the DODAG Information Object (DIO) signals to kick off the creation of DODAG. This created DODAG is advertised via link-local broadcast. The DIO messages provide details on the root identification of DODAG, the employed routing parameters, and the depth/rank of the generating router. The gateway that adopts the DODAG establishes its own rank based on the data published by its neighbors inside their DIOs [4].

RPL is an IPv6-based routing protocol for LLNs. There are no phases available since the technique is being used by network devices that are connected in this trend. The Destination Oriented Directed Acyclic Graph (DODAG), which itself is channeled to a specific destination, is constructed for this goal. This particular node is known as a

DODAG core in the RPL standard. The routing metric is defined by an Objective Function (OF) that is used to build the network. In other terms, the OF describes how to structure a building taking into consideration traffic limitations and other functionalities [6].

II. VERSION NUMBER ATTACK

A wide range of assaults that fall into three broad categories can be made against the RPL protocol. Attacks aimed at depleting network capacity fall under the first type (energy, memory and power). Such assaults are particularly harmful to such limited networks since they significantly reduce the gadget lifetimes and hence the RPL system lifetimes. Attacks that target the RPL network architecture fall under the second type. The architecture may be less optimal than it would be during a typical network converging, or a group of RPL units might well be cut off from the rest of the system, disrupting regular network functioning. The third category relates to assaults on internet activity, such as spying and theft assaults [8].

Version number assaults fall under the first group and have the potential to drastically shorten an IoT network's lifespan. As part of the method's immune response, they may be carried out at a little cost to the offender and make use of the universal maintenance process to overwhelm the system. When there are too many connectivity irregularities, the root starts a global repair. It entails recreating the whole DODAG by raising the DODAG's version number [7].

This number is included in control messages of the DODAG Information Object subtype (DIO). Every receiver of information contrasts the version number it now has with the one it acquired from its parent node. This must disregard its existing rank information, reset cascade timers, and start a new process to join the DODAG when the received version is greater. Although it is relatively expensive, this worldwide maintenance process ensures a topology without loops. The node did not upgrade to the latest iteration of the DODAG if the version displayed in DIO messages had an old value. Other nodes shouldn't select this component as their parent node. During universal maintenance, two copies of a DODAG may coexist[8].

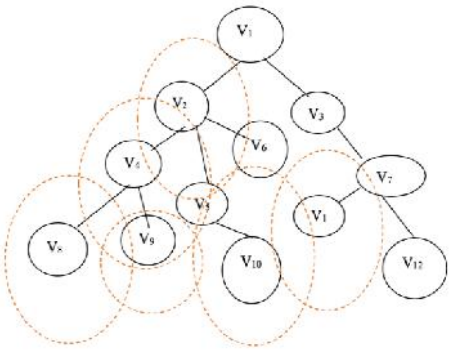

Figure 2.1: Version Number Attack [8]

III. LITERATURE REVIEW

Madakam, S., et al. in [1] concluded that a range of technologies and uses, IoT has already been progressively introducing a sea of changes in technology into our everyday lives, which then in turn contributes to making our lives easier and more comfortable. IoT applications are extremely beneficial in all fields, covering healthcare, manufacturing, industry, transport, educational, government, geology, and habitat, among others. Despite the many advantages of IoT, its administration and execution both have major shortcomings. The main takeaways from the literary works are as follows: That there's no strict definition in global, Worldwide standardizations are required in architectural level, Techniques are varying from seller, so requires to be inter - operable and For good international governance, humans need to build network protocol. Hope for improved IoT in the future.

Arış, A., et. al in [9] suggested two VNA prevention approaches, each with a distinct efficiency outcome and energy demand. The first mitigating method gets rid of VN modifications arriving from the leaf nodes' route. It ensures that the VNA's strongest positions are reduced in this manner. It cannot, nevertheless, lessen the impact of the onslaught on the remaining assaulting locations. As a result, the researchers consider a second mitigation strategy to lessen the impact of the assault regardless of the direction of the attacker. The second method only permits a cluster to modify its VN whenever the large bulk of its neighbours having higher rankings do so. On four different configurations, the reduced efficacy of the suggested methods is assessed. The findings demonstrate that using the suggested strategies can lessen the attack's negative consequences while still enabling valid Version Number upgrades. From this research, several things could be accomplished in further studies. One of these is the examination of the case involving several Version Number offenders, which hasn't yet been taken into account in the literature. Analyzing the effectiveness of a mixed mitigation

strategy is yet another problem. The Elimination strategy may be used on the networks with the least capabilities if the system has a dense architecture and variable node capabilities, and the Shield method may be used on the remaining nodes. Or, a cluster may choose to switch between Shields to Elimination depending on the amount of battery capacity left. The inclusion of movement, which may modify the nodes' ranks and the architecture constantly and may impact how well attack prevention works, is yet another thing to take into account.

Alshehri, F., & Muhammad, G. in [5] concludedthat a study has been done on smart healthcare. There is a wealth of literature in the field of smart health care that covers IoT, IoMT, clinical signals, AI, edge, and cloud services at different rates and using different strategies. To the best of understanding, there hasn't been a comprehensive review of the state-of-the-art IoT, IoMT, AI, utilization and fusion of medical signals, periphery and cloud technology, confidentiality, and cybersecurity in the field of smart health care. In order to provide a formal classification and particular comparison perspective for IoT, IoMT, AI, edge and cloud hosting, security and privacy in intelligent health care, this study sought to do just that.

García, S. N. M., et al. in [16] suggested a certification program for the internet of things. The test-based risk evaluation phase received emphasis in the suggested design. This approach was carried out to give researchers the ability to evaluate the security limitations for numerous internet of things setups. The presented solution was built using a few tools for analyzing safety and estimating danger in the IoT space. Numerous tests were run to evaluate various security concerns. The suggested method would later serve as a foundation for the creation of an innovative security categorization and accreditation method of internet of things elements.

Yoon, S., & Kim, J. in [15] suggested a brand-new, well realised building elements for a server that handles remote security. This strategy was put forth to guarantee the security of Connected devices in a handling situation. The distant vulnerability management server maintained and offered a variety of safety limitations in an interconnected and organized manner. The suggested method enabled to foreseeably prevent a number of negative events in the IoT scenario. The damage brought on by these assaults could be reduced with the detection of these attractions. In the eventuality that an attack occurs, the preventative steps could be used. The results of the numerous tests showed that the proposed method did well on key criteria, such as safety and security.

Mayzaud, A., et. Al in [10] provided a detection approach using specific algorithms to counter version number assaults in RPL systems. Relying on the edge network design, that protects limited node capabilities, the authors have implemented this approach. The base localizes the hacker after aggregating recognition data from all monitoring nodes, and the researchers have taken advantage of this teamwork to locate the hacker. They tested their idea with tests and assessed the results using predetermined criteria. They have demonstrated that a well-placed surveillance node may lower the rate of false positives of our approach. The researchers have taken into account the problem of scalability by putting forth an optimization problem that is simply adaptable to various architectures. By finding a solution to this issue, the authors have determined the precise number of processes of the organization needed to guarantee a reasonable probability of detection for a specific topology design.

Khan, Z. A., & Herrmann, P. in [12] suggested a few innovative IDS strategies that are ideal for small devices. The suggested strategy made use of the trust management method to handle the neighbors' updates. The suggested method worked extremely well at identifying evil-acting units. The procedure was carried out in a power-focused environment. The identification of the state's malicious node was indeed the primary goal of the subjectively logic used in trust maintenance. Three new variables—belief (b), disbelief (d), and uncertainty (u) -- that are based on assessments of both positive and negative trust have been added

$$b = \frac{\mathrm{p}}{\mathrm{p}+\mathrm{n}+\mathrm{k}} \quad d = \frac{\mathrm{n}}{\mathrm{p}+\mathrm{n}+\mathrm{k}} \quad u = \frac{k}{p+n+k}$$

The malicious node was removed from the internet after being identified. The three different RPL protocol assaults may all be successfully countered by the suggested technique. The suggested strategy might be used to different kinds of inclusions. In the coming years, a test bed containing Z1 components will be constructed for the verification of MATLAB computations. In this study, three distinct algorithms—Neighbour Based Trust Dissemination (NBTD), Clustered Neighbour Based Trust Dissemination (CNTD), and Tree Based Trust Dissemination—have being taken into consideration for controlling reputation (TTD).

Głowacka, J., et. al in [13] concluded that the knowledge of IoT nodes were produced by the authors using a cognitive method based on trust. Using this information, a suitable response to the possible hazards was also offered. The simulation findings for the antagonistic nodes indicated accurate identification, and in a tactical operations environment, the TUBE system's overall effectiveness was

assessed. It was also observed that this suggested technique effectively averted the reputational attacks that were induced by the existence of hostile items. The present method was tested in partially mobile circumstances with IEEE 802.11-based devices, and the findings were extremely effective.

Nitti, M., in [19] presented a study that concentrated on developing a dependable system that relies on object behavior in order to address the difficulties in comprehending how the data provided by individuals can be handled. Two management-effective methods are defined here, starting with those created for P2P & social platforms. With the use of a biased model, it is possible to determine the reliability of a node's connections depending on the node's individual perspective and the opinions of acquaintances who have comparable prospective network operators. With the use of an order for things, the data from each node is spread and then saved so that a disseminated hash table architecture may be created, allowing any other node to use similar data. The simulated findings demonstrated that practically any rogue station may be effectively separated from of the system by boosting network activity in return for information.

Abdul-Ghani, H. A., et. al in [14] suggested an approach was to overcome the version number assault problems in the RPL network. For the exchange of node resources, a distributed surveillance design-based solution was put into practice. In the suggested method, the cooperation of monitored nodes was taken advantage of to identify the attacker. The attacker carried out the intruder localization operation after collecting the recognition data from all surveillance nodes. Numerous tests were run to assess the effectiveness of the aforementioned strategy. The rate of false positives could be lowered with the aid of strategically placed monitoring nodes. Additional studies will include many more complimentary ones based on actual architecture and utilizing various additional classes of elements.

Guo, J., & Chen, R. in [17] concluded that IoT technologies have been found to connect billions of intelligent items to one another and the physical world. Such extensive interconnectedness among all objects has had a significant economic impact. Recently, the IoT devices that encourages to the other IoT components in the system have had misbehaving owners that must be dealt with in order to produce trust computing in IoT scenarios and increase their security. The firmly believed models that have been proposed up to this point are listed below. The existing trust computation models were categorized based on five design criteria: trust composition, trust propagation, trust aggregation, trust updating, and trust generation. The advantages and disadvantages of each dimension option were outlined, and the efficacy of defence mechanisms against a number of malicious attacks was emphasized. Through this study, the efficacy of trust computation approaches was presented, along with a list of the greatest and worst known trust calculation techniques. The holes in IoT firmly believed research were identified in the end, and some potential future directions were also suggested.

Bao, F., et al. in [21] proposed a revolutionary method that was highly adaptable, reliable, and extensible for changing IoT contexts. Because the objects in an IoT system were classified by the social networking sites of entity proprietors, a collection of interests (COI) due to social IoT was deployed. A reliable protocol with attributes like dependability, convergent, dynamics flexibility, and other properties was required attributed to the prevalence of constantly changing situations and malevolent nodes that carried out trust-related assaults. The proposed system's validity was demonstrated using both ideal and constrained storage areas. According to the results of the numerous experiments, the suggested trust management protocol, which uses a little amount of storage space, worked well and displayed strong adaptability and convergent.

Chen, R., et al. in [18] presented a method for adaptive trust management that would allow social relationships between IoT device owners to change over time. The design trade-off between trust resolution and trust variation was demonstrated inside the dynamic trust evaluation protocol architecture. A social IoT application utilizing adaptive trust based protocol was used to pick the appropriate trust parameter setting in regard to the changing IoT social settings in order to ensure that precision of trust management is good in addition to the increase of performance. Here, a bar counter method was used to analyse the data and demonstrate that the suggested adaptive trust evaluation mechanism was workable, proving that the proposed technique performed better.

Zarpelão, Bruno Bogaz, et al. in [20] examined the IoT system enhancement research that has been done in IDS well over years. Through this review, several issues, potential future developments, and current alterations were highlighted. The different IDSs were characterized in this study based on several key characteristics like verification, safety, IDS deployment method, and detection method. Here, the many scenarios for each attribute were reviewed to help determine whether the specific IDS schemes could be applied to IoT systems or how they could be utilised as attack detection skills to support the system safe.

Liu, Y., et al. in [22] suggested a model focused on the identification of node behavior, the trust management

framework. In the Internet of Things, received data was done using this approach (IoT). This approach made use of a trust record queuing with an unsigned integer trust model and harmful monitoring that might record the nature of the trust assessment. The test results showed that this model would work well for identifying malevolent noses that exhibited unusual behavior. Because this approach uses less store space and reduces communication costs between nodes, it has also proven useful for trust computing. As a result, the concept of applying evaluated for protection from inside attacks was quite beneficial.

IV. RESEARCH METHODOLOGY

The Research Methodology followed a theoretical approach of RPL, Trust-Based Mechanism and their comparative study on parameters. The selection of techniques for the objective includes literature survey, articles, books, research papers and internet.

Trust-Based Mechanism

In a community-based social IoT context [11], a trust evaluation protocol based on social trust updates the trust model by utilizing both direct observations and indirect suggestions.

- **Direct Trust Observations**

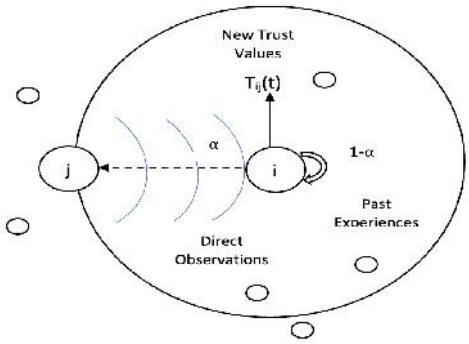

Figure 4.1: Node *i* evaluates node *j* with direct observations and past experiences.

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

x:Cooperativeness and honesty.

$T_{ij}^{honesty,direct}$: It is the disbelief of node *i* that node *j* is honest-based on node *i*'s direct observation towards node *j*.

$T_{ij}^{cooperativeness,direct}$: It provides the level of node *j*'s cooperation with *i* depending on first-hand observations across the range [*0, t*].

Δt: It is the time taken since the last trust update.

$1-\alpha$: It is the past experiences of node *i* towards the node *j*.

$T_{ij}^{x}(t)$: It is the new trust value of node *i* towards the node *j*.

- **Indirect Trust Observations**

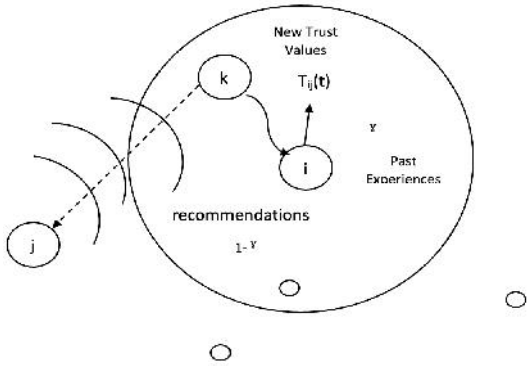

Figure 4.2: Node *i* evaluates node *j* with recommendations from node *k* and past experiences.

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

T_{ik}^{X}: It is the Trust Value of node *i* towards the recommender node *k.* Contribution of recommended trust increases proportionally as either T_{ik}^{X} or β increases.

i: It is the assigned weight to current trust.

βT_{ik}^{X}: It is the weight assigned to new recommendation.

γ: It is the past experiences of node *i* towards node *j*.

$1-\gamma$: These are the recommendations of node *k* towards node *j*.

$T_{ij}^{x}(t)$: It is the new trust value of node *i* towards node *j*.

Proposed Algorithm

Input: Sensor Nodes
Output: Detection of Malicious nodes

i. Construct a network with a limited amount of sensor nodes i.e., 38.
ii. Organize the whole network in to fixed-size clusters.
iii. Depending on the range and energy usage, choose the cluster head for every cluster.
iv. Calculate Trust
   a. Check number of packets transmitted by the sensor node
   b. Number of packets forwarded is calculated by equation below

*TPF=Port Number*Corresponding Packet Forwarding Rate of Packets*

   c. The PDR is calculated by the equation given below

$$PDR = \frac{Number\ of\ packets\ received}{Number\ of\ packets\ sent} \cdot \frac{1}{P_{TPF}}$$

   d. PDR define the total number of packets forwarded in the network by the source node.
v. If (PDR < Threshold PDR)
vi. Declare the sensor node malicious.
vii. Create a new route from the origin to the endpoint.
viii. Send data using the previously chosen route.

End

V. RESULTS

The simulation is performed to evaluate various performance metrics like Packet Loss, Latency and Control Message Overhead. These metrics are evaluated by comparing their performances when the Version Number attack is implemented into the simulated environment. The simulator used is NS2 Version: 2.35. The total number of nodes that are injected into the 800*800 environment are 38 nodes.The antenna type is Omni-Directional as it radiates equal radio power in all the directions perpendicular to an axis and the channel is wireless as WSN uses wireless channels for propagation. It is simulated on the system having Ubuntu 18.04, core i-5 processor and 8GB of Ram.

Given below are the results on the basis of various parameters and values

Parameters	Values
Simulator	NS2 Version: 2.35
Nodes	38
Area	800*800
Antenna Type	Omni-Directional
Channel	Wireless
Propagation Model	Two-Ray
Operating System	Ubuntu 18.04
Processor	Core i5
RAM	8 GB

Parameters selected for evaluation

- **Packet Loss**

The metric known as Packet Loss calculates how many packets are dropped throughout the transmission of data. When the Version Number attack is triggered into the simulated environment, the packets are analyzed in terms of bytes on the basis of Attack Scenario, Existing Technique and Proposed Work. The performance is evaluated on the various time frames taken in seconds.

Time(in Sec)	During Attack	Existing Technique	Proposed Work
2	0.6	0.25	0.05
4	1.15	0.49	0.19
6	1.28	0.55	0.30
12	1.29	0.57	0.42
14	1.30	0.56	0.45

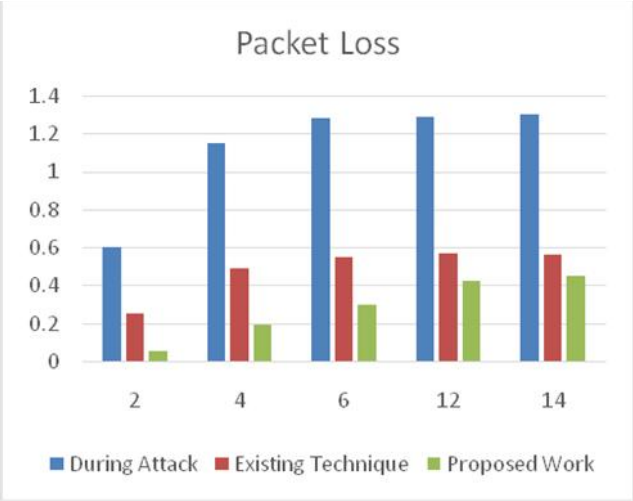

Figure 5.1: Packet Loss Analysis.

The Attacks Scenario had the highest number of packet loss, according to analysis. Following that, packet loss is decreased in the Existing Technique compared to the Attack Scenario. However, the Proposed Strategy reduces packet loss to a minimum but not to zero.

- **Latency**

A network's latency describes how long it would take for a piece of data to go from one node or terminal to the other from across channels. The latency is calculated when the Version Number attack is triggered into the simulated environment in terms of bytes on the basis of Attack Scenario,

Existing Technique and Proposed Technique. The performance is evaluated on the various time frames taken in seconds.

Time(in Sec)	During Attack	Existing Technique	Proposed Work
2	0.59	0.30	0.05
4	1.13	0.57	0.19
6	1.26	0.63	0.30
12	1.28	0.64	0.43
14	1.30	0.65	0.47

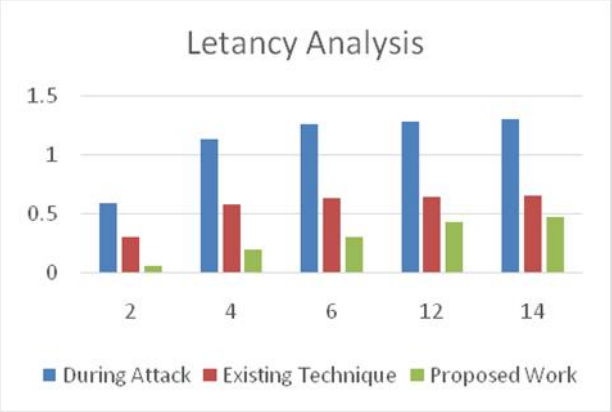

Figure 5.2: Latency Analysis.

According to analysis, the attacks scenario have seen the greatest latency. After then, latency in the existing work is shorter than the attack situation. However, the proposed approach minimizes the latency while not totally eliminating it.

o Control Message Overhead

It is the time consumed doing an indirect calculation that uses storage, connectivity, or even other resources. The above parameter is also calculated when the Version Number attack is triggered into the simulated environment in terms of packets on the basis of Attack Scenario, Existing Technique and Proposed Technique. The performance is evaluated on the various time frames taken in seconds.

Time(in Sec)	During Attack	Existing Technique	Proposed Work
4	200	60	160
6	770	230	240
12	930	570	530
14	940	670	570

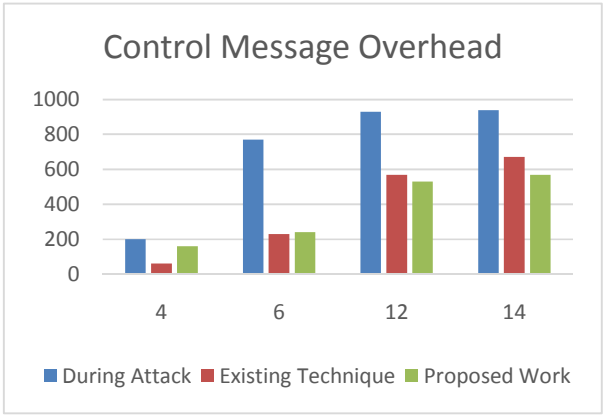

Figure 5.3: Control Message Overhead Analysis.

According to the results, the Control Message Overhead remained slightly higher in the beginning, specifically in the fourth and sixth seconds, as compared to the existing work. The Control Message Overhead, however, dropped as the time scale grew, and it was lowest in the proposed technique. The simulated environment has been most heavily affected by the Control Message Overhead during the attack.

VI. CONCLUSION

The research mentioned above relates to the identification of a Version Number attack in an IoT simulation environment. It makes advantage of DODAG, a hierarchical architecture for RPL that raises the Version Number. In the research paper mentioned above, a proposed methodology is developed to identify hostile nodes in the network. The NS2 software simulates the aforementioned method utilizing 38 network nodes spread across an area of 800*800 meters. Analysis shows that the simulation reduces both packet loss and latency. However, the Control Message Overhead rises at first then falls as the time frame increases. The Proposed Strategy outperformed the other two ways, during the Attack Situation and the Existing Method.

REFERENCES

[1] Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.

[2] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In 2012 10th international conference on frontiers of information technology (pp. 257-260). IEEE.

[3] Alkhatib, H., Faraboschi, P., Frachtenberg, E., Kasahara, H., Lange, D., Laplante, P., ...& Schwan, K. (2015). What will 2022 look like? The IEEE CS 2022 report. Computer, 48(3), 68-76.

[4] Balaji, S., Nathani, K., & Santhakumar, R. (2019). IoT technology, applications and challenges: a contemporary survey. Wireless personal communications, 108(1), 363-388.

[5] Alshehri, F., & Muhammad, G. (2020). A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. IEEE Access, 9, 3660-3678.

[6] Soumyalatha, S. G. H. (2016, May). Study of IoT: understanding IoT architecture, applications, issues and challenges. In 1st International Conference on Innovations in Computing & Net-working (ICICN16), CSE, RRCE. International Journal of Advanced Networking & Applications (No. 478).

[7] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, IETF, 2012.

[8] Souri, A., Hussien, A., Hoseyninezhad, M., & Norouzi, M. (2022). A systematic review of IoT communication strategies for an efficient smart environment. Transactions on Emerging Telecommunications Technologies, 33(3), e3736.

[9] Arış, A., Yalçın, S. B. Ö., & Oktuğ, S. F. (2019). New lightweight mitigation techniques for RPL version number attacks. Ad Hoc Networks, 85, 81-91.

[10] Mayzaud, A., Badonnel, R., & Chrisment, I. (2016, October). Detecting version number attacks in RPL-based networks using a distributed monitoring architecture. In 2016 12th International Conference on Network and Service Management (CNSM) (pp. 127-135). IEEE.

[11] Bao, F., & Chen, I. R. (2012, September). Dynamic trust management for internet of things applications. In Proceedings of the 2012 international workshop on Self-aware internet of things (pp. 1-6).

[12] Khan, Z. A., & Herrmann, P. (2017, March). A trust based distributed intrusion detection mechanism for internet of things. In 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA) (pp. 1169-1176). IEEE.

[13] Głowacka, J., Krygier, J., & Amanowicz, M. (2015, December). A trust-based situation awareness system for military applications of the internet of things. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) (pp. 490-495). IEEE.

[14] Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. (2018). A comprehensive IoT attacks survey based on a building-blocked reference model. International Journal of Advanced Computer Science and Applications, 9(3).

[15] Yoon, S., & Kim, J. (2017, October). Remote security management server for IoT devices. In 2017 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1162-1164). IEEE.

[16] García, S. N. M., Hernandez-Ramos, J. L., & Skarmeta, A. F. (2018, February). Test-based risk assessment and security certification proposal for the Internet of Things. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 641-646). IEEE.

[17] Guo, J., & Chen, R. (2015, June). A classification of trust computation models for service-oriented internet of things systems. In 2015 IEEE International Conference on Services Computing (pp. 324-331). IEEE.

[18] Chen, R., Bao, F., & Guo, J. (2015). Trust-based service management for social internet of things systems. IEEE transactions on dependable and secure computing, 13(6), 684-696.

[19] Nitti, M., Girau, R., & Atzori, L. (2013). Trustworthiness management in the social internet of things. IEEE Transactions on knowledge and data engineering, 26(5), 1253-1266.

[20] Zarpelão, Bruno Bogaz, et al. "A survey of intrusion detection in Internet of Things." Journal of Network and Computer Applications 84 (2017): 25-37.

[21] Bao, F., Chen, R., & Guo, J. (2013, March). Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In 2013 IEEE eleventh international symposium on autonomous decentralized systems (ISADS) (pp. 1-7). IEEE.

[22] Liu, Y., Gong, X., & Xing, C. (2014, August). A novel trust-based secure data aggregation for internet of things. In 2014 9th International Conference on Computer Science & Education (pp. 435-439). IEEE.