Secure Inter-Domain Routing for Resisting Unknown Attacker in Internet-of-Things

Bhavana A[1]
Research Scholar, Department of Computer Science and Engineering, VTU, Belagavi
Karnataka, India

Nanda Kumar A N[2]
Professor, Department of Computer Science and Engineering, City Engineering College
Bangalore, India

***Abstract*—With an increasing adoption of Internet-of-Things (IoT) over massively connected device, there is a raising security concern. Review of existing security schemes in IoT shows that there is a significant trade-off due to non-adoption of inter-domain routing scheme over larger domain of heterogeneous nodes in an Internet of Things (IoT) via gateway nodes. Hence, the purpose of the proposed study is to bridge this trade-off by adopting a new security scheme that works over an inter-domain routing without any apriori information of an attacker. The goal of the proposed framework is to identify the malicious intention of attacker by evaluating their increasing attention over different types of hop links information. Upon identification, the framework also aims for resisting attacker node to participate in IoT environment by advertising the counterfeited route information with a target of misleading the attackers promoting autonomous self-isolation. The study outcome shows proposed scheme is secure compared to existing scheme.**

Keywords*—Internet-of-things; security; inter-domain routing; gateway node; attacker

I. Introduction

Internet-of-Things (IoT) is one of the evolving technologies toward data acquisition and controlling of large number of objects, digital and mechanical machines, computing devices, etc. without any form of dependencies toward human intervention [1]. Owing to the connection of different types of devices (or machines), there is an increasing security threats [2]. The first security threat in IoT device is inappropriate access control due to usage of same default password as the underlying firmware basically runs a default setting of all IoT devices of same model [3]. The second prominent threat is there is a larger base of attacker as different number of machines is connected over internet with an open port [4]. As IoT has an inclusion of large number of connected machines so eventually it suffers from regular updating of software. Conventional IoT device doesn't uses sophisticated encryption process and hence it gives rise to man-in-middle attack and denial-of-service attack in IoT [5]. Absence of reliable and trusted operating environment is another reason behind the security threat which often gives rise to privacy preservation issues. Due to usage of large number of machines, it is less feasible to offer reliable physical security towards IoT device. Apart from this, the conventional IoT nodes perform communication using various types of routing protocols [6] while Datagram Transport Layer Security (DTLS), Internet Protocol Security (IPSec), and Routing Protocol for Low-Power and Lossy Networks (RPL) are known to offer security. However, there are different ranges of literatures which have reported of security pitfalls in existing routing protocols in IoT. Out of all this, one elementary concern is that IoT which runs on heterogeneous nodes doesn't seem to consider adopting inter-domain routing protocols. At present, there are such protocols reported to work over internet, however, they were never meant to be functional over IoT architecture, which is more complex form of architecture to be used in Future Internet Architecture [7][8]. Some of the challenges of implementing inter-domain routing scheme in IoT are as follows: i) developing a routing strategy among different forms of devices with multiple roles is definitely not an easy task considering the massiveness of the network, ii) developing both centralized as well as decentralized trusted authority connected to gateway node in IoT is one of the tedious task to be accomplished, iii) existing firewall system in IoT application is dependent on definition of patch and hence they are incapable of identifying new form of threats that are not defined in firewall system, iv) usage of conventional encryption process also comes with different forms of operational and communication challenges over resource constrained IoT devices [9]. All the above reasons serves as a motivation factor as well as reason towards develop a robust security protocol which is compliant of inter-domain routing as well as which is computationally efficient for practical implementation of complex environment of an IoT. The primary objective of the proposed manuscript is to introduce a novel solution where hop-based behaviour for all the nodes are observed to identify the malicious intention of attacker node, assuming its originality is unknown to the system. The secondary objective of proposed study is to resist attack in the form of novel inclusion of guard node. This new variant of node is meant to offer forged information of routes to attacker node in order to force them to accept the wrong direction of data dissemination. The objective of this operation is to ultimately results in either exclusion of attacker or their complete drainage of resources.

The organization of this manuscript is as follows: Section II discusses existing literatures of secure communication in IoT followed by discussion of research problems that are identified to be addressed in proposed study in Section III and proposed solution towards resisting unknown threat using inter-domain routing in IoT is briefed in Section IV. Section V discusses about algorithm design and implementation for secure route formulation and resisting malicious node participation followed by discussion of result analysis in Section VI. Finally, the conclusive remarks are provided in Section VII.

II. Related Work

This section presents a briefing of the existing research implication being carried out towards securing communication in IoT as a continuation of our prior study [10]. The recent study carried out by Yilmiz et al. [11] have presented a discussion of a machine learning approach for securing IoT device using Routing Protocol for Low-Power and Lossy Network (RPL) protocol. Yazdinejad et al.[12] have used blockchain-based method for securing software defined network in IoT in the form of clustering. Study towards prevention of intrusion event is carried out by Haseeb et al. [13] considering the case study where sensors are used in IoT considering multi-hop routing and blockchain-based scheme. The work of Mick et al. [14] has presented a unique authentication scheme considering named data networking adhering to the concept of hierarchical routing. The work carried out by Xu et al.[15] have presented a secure routing scheme for resisting jamming attacks in IoT using game theory for exploring the optimal secure path for data delivery. Raoof et al.[16] have presented discussion of existing threats and countermeasures exclusively towards frequently used RPL protocol in IoT. Haseeb et al. [17] have presented a security scheme where secret shares has been used for data communication with energy efficiency. Usage of reinforcement learning scheme has been noticed in work of Guo et al. [18] to ensure balance between security and quality of service at same time. Raoof et al.[19] have presented an improved security scheme for RPL when subjected to different forms of attacks in IoT. The work carried out by Shin et al.[20] have developed an optimization mechanism for routing process in IoT focusing on securing authentication process. Wadhaj et al.[21] have developed a preventive technique towards attack on IoT device using RPL protocol with a target to maximize the reliability score of attacker identification process. Saleem et al.[22] have used a bio-inspired approach towards securing IoT communication over 5G. Ramos et al.[23] have carried out an investigation toward analyzing security aspects of resource-constrained IoT devices using probabilistic model. Liu et al. [24] have implemented a scheme towards resisting sink hole attack in IoT using probing routes considering consumption of network energy. Usage of geometric-based communication scheme anonymously is presented by Sun et al.[25] where hashing-based encryption has been utilized to ensure data privacy. Haseeb et al.[26] have presented a trust-based security scheme for mesh network in IoT considering cost of link and dissemination of data. Similar scheme has been carried out by Jhaveri et al.[27] towards trust-based security in IoT focusing on identifying the pattern of attack. Sathyadevan et al. [28] have introduced an authentication scheme using key generation technique exclusively meant for edge computing IoT device. Trust-based security scheme using provisioning approach was presented by Dass et al. [29] considering transport system in IoT. Agiollo et al. [30] have presented a unique scheme of identification of routing attack when standard RPL is deployed in IoT. Hence, there are different variants of security scheme toward safeguarding communication system in IoT. A closer look into all the above research implication has proven its substantial benefits from security perspective; however, they are highly symptomatic in nature of attack and is also associated with various limitation. The next section outlines the identified research problem from the above stated literatures.

III. Research Problem

The discussion of the research problem is carried out with respect to observed limitation and research gap as briefed below:

A. Limitation

The limitations that have been identified in proposed study are as follows:

- Existing security techniques towards IoT mainly uses either trust-based, or machine learning, or block chain in increasing pattern, which are sophisticated process for low resource IoT device.
- All the existing schemes has a well definition of attack and their strategy to initiate an attack is well known prior implementing security scheme.
- There are no reported study towards identification of threats on the basis of hops and malicious behaviour of attackers in heterogeneous nodes in IoT.
- There are no reported inter-domain routing scheme in IoT apart from the standard routing scheme which are exercised from long time.

B. Research Gap

The prime research gap of existing system is that with an increase of dynamicity and uncertainty in attack behaviour, existing security solutions over an IoT are yet not equipped to meet security demands both from hardware, software, and network perspective. The prime justification behind this research gap is that-it can be seen that there are various ranges of literatures that emphasize towards resisting attacks in IoT system, however, their work is not carried out over inter-domain routing system. This will be the prime reason that existing models are just theoretical model with theoretical proof of concept. The moment, such models are implemented over a gateway node, there is a need of a drastic revision towards such model in terms of network configuration as well as threat modelling. Hence, there is a vast gap between the security demands and the conclusive claims of existing studies.

Therefore, the problem statement of the proposed study can be stated as “Identifying an unknown attacker and resisting them in large IoT heterogeneous network using inter-domain routing scheme is quite a challenging task”. The next section discusses about the solution towards this problem.

IV. Proposed System

The proposed study is a continuation of our prior framework of inter-domain routing with scalability [31] and interoperability [32] which offers a concrete baseline of two heterogeneous domains and wireless nodes within it to communicate via base station in IoT. The proposed system introduce security on the top of the previous framework for two purpose viz. i) to offer secure communication among communicating nodes and ii) to prevent any form of malicious nodes participating in data dissemination process. The

architecture of proposed system is as shown in Fig. 1. The core ideology of proposed secure inter-domain routing scheme is that every IoT device is communicated via a relay node controlled by base station which mainly broadcast hello message and instructions to control the topology. Hence, it becomes important for system to safeguard such relay nodes as well as other regular IoT nodes. The core operation is classified into secure route formulation and preventing attackers node to join the network on the basis of evaluation of links and control messages. A target node (exploited node) is assessed using primary and secondary rule to find out if they are completely compromised or could have feasibility to be secured. Further, all the double hop links are evaluated in order to find out presence of malicious nodes. The novelty of proposed system is the formulation of guard node which is meant for preventing the malicious node from participating in data forwarding process. The next section of the paper elaborates about the algorithm design and implementation towards secure inter-domain routing in IoT.

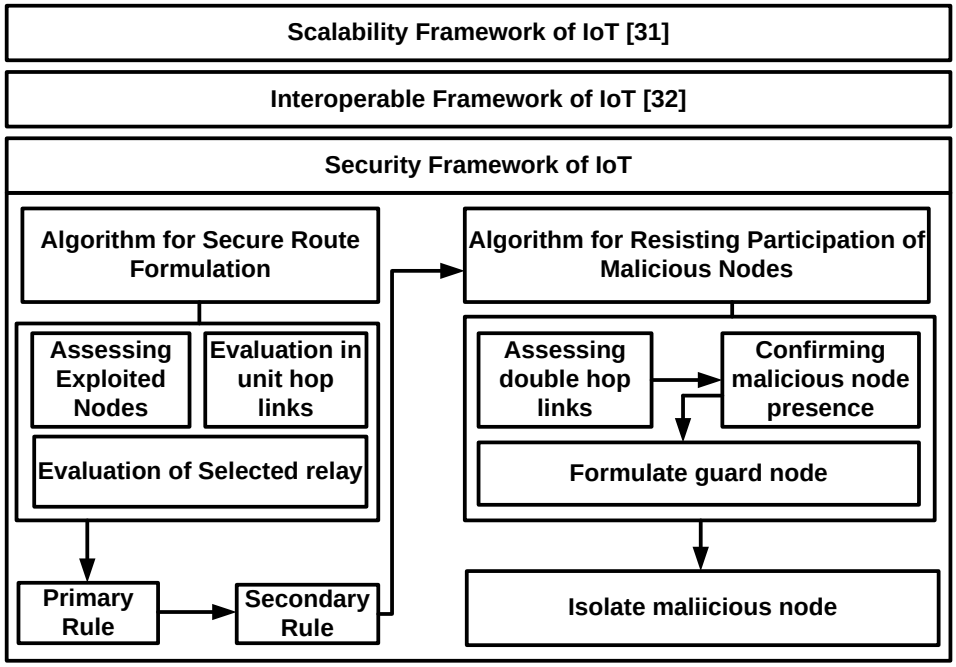

Fig. 1. Proposed Architecture of Secure Inter-domain Routing in IoT.

V. Algorithm Implementation

This section discusses about the algorithm design used for securing the proposed inter-domain routing system focusing on IoT use case [31] [32]. It should be noted that both these framework has already offered scalability as well as interoperability features while performing data transmission. This part of implementation focusses on embedding secure communication of inter-domain routing among all the participating nodes in IoT. The complete algorithm implementation is carried out using two discrete modules i.e. securing route formulation and resisting participation of malicious node. The description of algorithms design is as follow:

A. Algorithm for Secure Route Formulation

The main purpose of this algorithm is to initiate a secure topology in inter-domain routing connecting all sorts of nodes with an emphasis towards the exploited node (or compromised node). However, the degree of exploitation is yet not ascertained prior to implementation of this algorithm and the basis task of this algorithm is also to restrict all the communication system with unit hops in order to prevent collateral spread of exploitation by the unknown malicious node. The algorithmic flow is shown in Fig. 2 and its steps are as follows:

Algorithm for Secure Route Formulation

Input: *n* (wireless nodes)
Output: M (matrix storing network information)
Start
1. **For** i=1:*n*
2. $x_7 \rightarrow bc(uh(x_7))$
3. Φ confirm $n_{dec}(x_7) \notin uh(\Phi)$
4. **For** j=1:α
5. Φ assess $\beta \in uh(\alpha)$
6. $\beta \notin bc(msg)$
7. $\beta \rightarrow (uh+2)\Phi$
8. **End**
9. M=[Φ β uh]
10. **End**

End

The algorithm takes the input of all the participating wireless nodes n which after processing should yield a matrix M that stores network information to be used further for secure routing. The algorithm implements two set of rules to offer security. The primary rule is that the node x_7 will broadcast bc a unit hop links of x_7 node (Line-2). In such case, the exploited node Φ is required to confirm that declaration given by node x_7 should not belong to unit hop links of itself i.e. $uh(x_7)$ (Line-3).

This is possible by evaluating the previous broadcast message to assess if they have declared the transmitting node as its adjacent nodes. It is necessary that node x_7 must choose relay node in double hop $dh(x_7)$ in order to reach all the nodes present in double hop i.e. x_1 and x_4. However, there is also a possibility that x_7 could opt for selecting Φ as its relay node in order to protect x_1 and x_4 nodes. Hence, according to security definition of non-repudiation, the node Φ is not permitted to deny the selection process. In such condition, the node Φ is incapable of confirming the fact if node x_7 is really an attacker node. However, it is feasible for the node Φ to assess if node x_7 has selected different relay node from the double hop links i.e. $dh(x_7)$ i.e. either x_2 or x_5 (Fig. 2). Therefore, a secondary ruleset is developed which states that if there is a presence of a different node α (Line-4) that is declared in the control message of inter-domain routing, than it is basic duty of the node Φ to find out if there is presence of some other new node say β which is already existing in unit hop links of α i.e. $uh(\alpha)$ (Line-5). It is also required to ensure that the node β is not declared in the transmitting message broadcasted (Line-6) as well as it is also required to ensure that this node β is positioned with a difference of three hops from the node Φ (Line-7). Once, this condition is evaluated, than the system undergoes another level of assessment which is to check if the node x_7 has selected some other new node which is a present in definition of unit hop links of node x_7 i.e. $uh(x_7)$ as relay node in order to protect other node β. All this information are stored in a matrix M (Line-9) which is consistently updated in every round of communication by the participating node. The core idea is to ensure that no unknown node is given the right to select some other undefined node from both the forms of link (unit/double) as the relay node.

The contribution of this algorithm are as following: i) a secure link is formulated among all the participating nodes, ii) multiple level of assessment is carried out to double-check the presence of relay node and its connection with all the adjacent nodes, iii) the algorithm is completely non-iterative and its information gets periodically updated in matrix M stating that there is a less computational complexity associated with it.

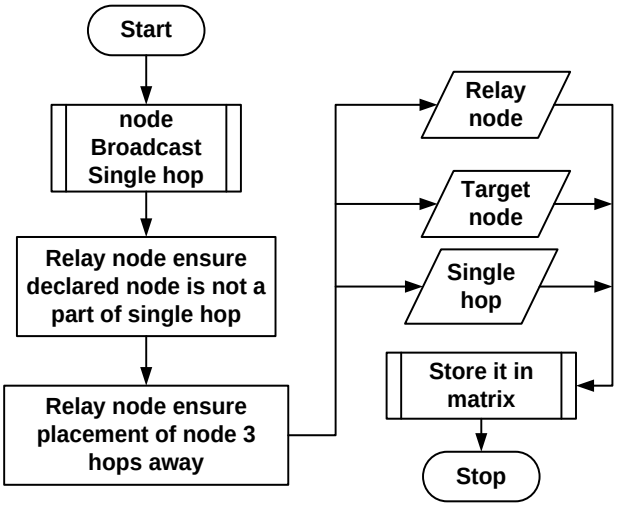

Fig. 2. Process Flow for Algorithm for Secure Route Formulation.

B. Algorithm for Resisting Participation of Malicious Nodes

This algorithm is basically responsible for confirming the presence of an unknown malicious nodes followed by a unique process of isolating them from the rest of the resured network formulated in matrix M. The core target of this algorithm is equivalent to first algorithm i.e. protecting the relay nodes from wrongly appointed by any attacker node. The prime concept underlying in this process is that attacker node is always curious to travel in doubl hop links in order to propagate their malicious code and the idea of this algorithm is to stop this process. The algorithmic flow (Fig. 4) and its respective steps are as follows:

Algorithm for Resisting Participation of Malicious Nodes

Input: Φ (exploited node), M (matrix of links)
Output: s_r (secure removal)
Start
1. **For** i=1:Φ
2. **For** *cond*=True
3. Φ add n_g
4. Ensure dist(α, β)< (uh+2)|M
5. $n_g \notin uh(\Phi)$
6. $\beta \rightarrow bc(n_g)$ & goto step-3
7. **Else**
8. remove n_g
9. flag $s_r \rightarrow$secure removal of malicious node
10. **End**

End

The prime ideology of this algorithm are as follows: i) the node x_7 should demand to know only the nodes which is advertised by unit hop links of Φ i.e. $uh(\Phi)$, ii) the node x_7 selects relay node in order to achieve coverage to nodes mentioned in double hop links i.e. $dh(x_7)=x_1, x_4, x_2, x_5, x_8$ etc. It will mean that node x_7 is likely not to opt for x_4 node as its relay node can reach node x_2 via node x_5 as shown in Fig. 3.

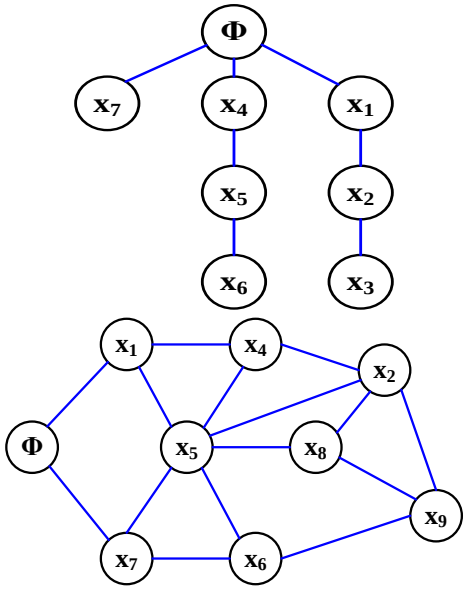

Fig. 3. Considered Test Topology.

The proposed algorithm formulates a condition cond (Line-2) which means for all the nodes β that is a part of dh(Φ) if there exist any node α that is an element of unit hop of Φ i.e. uh(Φ) (Line-1). Therefore, the algorithm selects a guard node ng to be added for all node Φ (Line-3) such that spatial distance among all the nodes i.e. α, β is less than 3 hops (Line-4) obtained from matrix M.

The algorithm also ensure that this guard nodes ng is not advertised by unit hop links of node Φ i.e. uh(Φ) (Line-5) in order to protect them from getting disclosed to attacker node. The node β starts declaring guard node ng as a regular node in order to attract the attention of attacker (Line-6). In this case, as the attacker is also obeying the policy of undeniability of service in proposed secure inter-domain routing, therefore, it has to agree on accepting the counterfeited route information provided by β. This causes the attacker node to explore all the nodes which doesn't exist as well as which are never mentioned in either of the unit/double hop links of β or Φ or x_7 node. By following the counterfeited routes, the attacker allocates all its resources to capture information of the nodes and it drains all its resources until it either chooses to leave the network or stays in the network until its resources are completely drained. At the same time, it is also required to eliminate the guard node identity from the advertised message after the work of transmitting the counterfeited message is accomplished in order to offer more security. It also prevents the attacker even to guess the formation as well as trend of guard node message especially in case of multiple attackers. Finally, a flag message of secured removal of malicious node is disseminated in the network reporting the identity of the attacker node that prevents the same attacker node to intrude the network. The next section discusses about result being obtained.

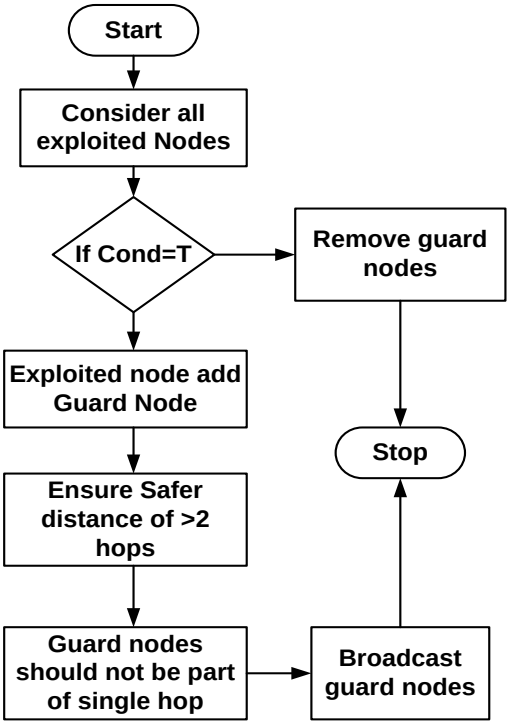

Fig. 4. Process Flow for Resisting Participation of Attacker.

VI. Result Analysis

This section discusses about the results obtained after implementing the proposed algorithm discussed in prior section. A simulation area of 1000 x 1000 m2 is used where 100 sample wireless nodes are deployed adhering to the inter-domain routing scheme [32]. The proposed logic is scripted in MATLAB where different test environment of undefined attacker is considered. The outcome of the study has been evaluated by different parameters. Table I and Fig. 5 highlights the frequencies of an attack event for 800 node density that clearly highlights the reduction of attack event with progressive density of nodes. The justification behind this outcome is that with more events of positively identified attacks, the routing tables gets updated which can be accessed via any gateway node to upgrade heterogenous domains under communication. Hence, the proposed system offers better control of malicious nodes in inter-domain routing scheme.

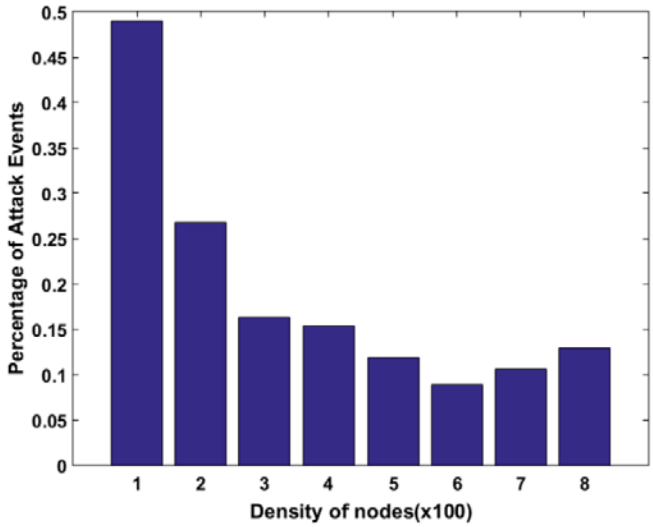

Fig. 5. Percentage of Attack Event.

TABLE I. Numerical Score of Attack Events

Density of Nodes	Percentage of Attack Events
1	0.489
2	0.275
3	0.17
4	0.15
5	0.13
6	0.09
7	0.11
8	0.14

The proposed system has been compared with existing security protocol in IoT Routing Protocol for Low-Power and Lossy Networks (RPL), which is claimed to offer balance between security and resource efficiency. The idea is to assess the control towards overhead as well as dependencies of guard nodes. Fig. 4 highlights that proposed system offers reduced overhead that is computed by every extra data being forwarded by the transmitting node. It is because although RPL offers great security but it suffers from long delays especially when

exposed to unknown form of attacks under node formation in tree. However, proposed system performs parallel confirmation of node legitimacy as well as data transmission causing reduced overhead.

Discussion: From the tabulated information as well as graphical data, it can be seen that proposed system is potential enough to control the attacker (Fig. 5) as well as it can also reduce the overhead (Fig. 6 and Table II). The significance of this outcome is quite high as usage of conventional scheme of IoT secure routing results in increasing overhead. When subjected to inclusion of multiple hardware in the form of network devices, it is quite inevitable that IoT device will incur more number of queued packets resulting in overhead. However, this is not the case with proposed scheme for two reason viz. i) all the hop information are basically shared among all the regular nodes and hence accessibility becomes easier, and ii) permission for data transmission is granted only after a node is confirmed to be a legitimate node in progressive round.

Fig. 7 and Table III highlights that proposed system offers reduced dependencies of guard node in order to prevent the malicious node as compared to existing protocol of RPL. Fig. 8 highlights the comparative analysis of processing time which shows that proposed system consumes much less time in contrast to existing RPL protocol.

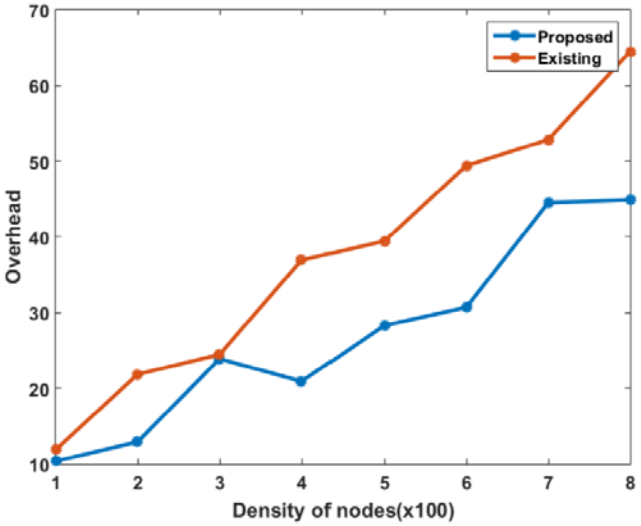

Fig. 6. Comparative Analysis of Overhead.

TABLE II. NUMERICAL SCORE FOR OVERHEAD ANALYSIS

Density of Nodes	Existing System	Proposed System
1	10.38	11.93
2	12.96	21.87
3	23.91	24.48
4	20.94	36.96
5	28.31	39.47
6	30.71	49.42
7	44.53	52.87
8	44.90	64.49

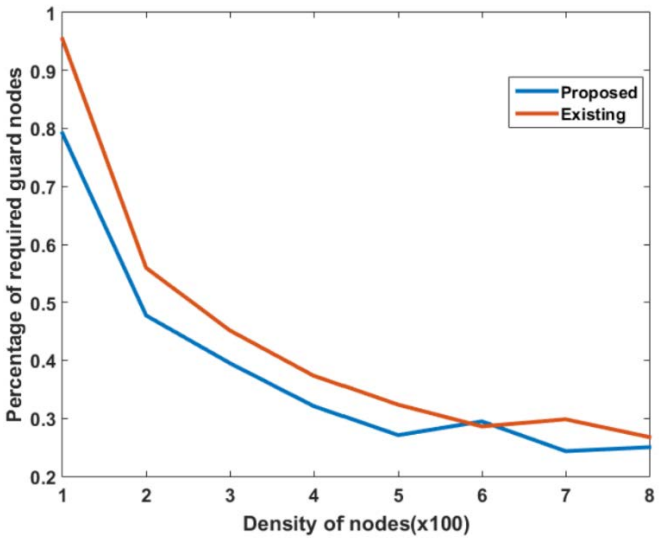

Fig. 7. Comparative Analysis of Percentage of Required Guard Nodes.

TABLE III. NUMERICAL SCORE FOR GUARD NODE DEPENDENCY

Density of Nodes	Existing System	Proposed System
1	0.7913	0.9539
2	0.4774	0.5594
3	0.3952	0.4516
4	0.3211	0.3735
5	0.271	0.3235
6	0.2947	0.286
7	0.2434	0.2983
8	0.2502	0.2677

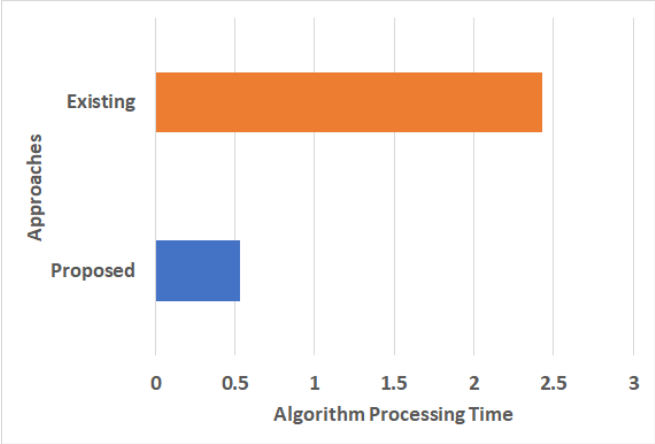

Fig. 8. Comparative Analysis of Algorithm Processing Time.

Discussion: The prime reason behind this outcome shown in Fig. 7 and Fig. 8 is as follows- because RPL protocol performs assessment of security instantly and performs secure encryption ignoring the fact that if the same attacker has compromised some other set of links in its far neighboring nodes. On the other hand, proposed system gather more information about attacker node via guard node and this gets updated in the form of matrix, which is easily accessible via gateway node. This causes the attacker node to completely

eliminate from network by spending all its resources towards counterfeited nodes advertised by guard node and if the same attacker or its connected attacker with multiple strategy is trying to launch an attack from different nodes. The proposed system easily captures that information via double hop links. Greedy attackers have more concentration of response towards double hop links and that makes the identification quite easier. It is seen that RPL completely works on directed acyclic graph without any edges outgoing. Apart from this, owing to inclusion of number of control messages used, there is a huge consumption of time especially when working on higher number of heterogeneous nodes. This causes much consumption of its time, whereas proposed system formulates a simplified logic of capturing the attacker intention via their response message over the dual hop links. Identification operation becomes much easier by accessing a single hand matrix for faster detection. Hence, proposed system can be considered almost instantaneous in offering its response time, which is an additional benefit from secure routing.

VII. Conclusion

This paper has presented a unique solution towards confirming the malicious intention of an attacker over proposed secured inter-domain routing in IoT. The summary of research findings are as follows: i) one prime indicator of an attacker node is to assess their intention to carry out routing from the nodes with maximum hop, ii) trust computation always works well when it is splitted to local trust and global reputation system, iii) acceptance of global reputation system should be followed by authenticating the legitimacy of the neighboring nodes, iv) updating hop table as well as limiting hop access is one of the safest means to restrict the propagation of uncertain threats. The summary of the proposed method are i) proposed method is capable of working over an inter-domain routing in presence of uncertain threat, ii) proposed model exploits the hop-based detailed information to formulate the attack possibilities as well as malicious intention, iii) proposed model offers robust security even without using conventional encryption process in IoT. The summary of contribution of the proposed system are i) it presents a novel architecture where secure inter-domain routing is implemented for resisting unknown attacker, ii) the complete analysis of malicious intention is based on attacker response towards different types of hops, iii) the framework also present an inclusion of a guard node which is meant for forwarding forged routing information to mislead the attacker node. The novelty of the proposed study are as follows: i) the model is independent of any form of attack definition unlike existing system which demands proper definition and types of attack, ii) a novel selection of relay node is developed unlike any secure routing scheme in IoT for topology control, iii) a completely non-encryption-based approach whereas majority of standard approaches uses cryptography.

References

[1] H. H. Qasim, A. E. Hamza, L. Audah, H. H. Ibrahim, H. A. Saeed, M. I. Hamzah, “Design and implementation home security system and monitoring by using wireless sensor networks WSN/internet of things IoT”, International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 3, June 2020, pp. 2617~2624.

[2] Shamshekhar S. Patil, Arun Biradar, “Novel authentication framework for securing communication in internet-of-things”, International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 1, February 2020, pp. 1092~1100.

[3] Mohammed Al- Shabi, Anmar Fakhri Abuhamdah, "Using deep learning to detecting abnormal behavior in IoT", vol.12, No.2, 2022, DOI: http://doi.org/10.11591/ijece.v12i2.pp%25p.

[4] Basheer Al-Duwairi,Wafaa Al-Kahla, Mhd Ammar AlRefai, Yazid Abdelqader, Abdullah Rawash, Rana Fahmawi, “SIEM-based detection and mitigation of IoT-botnet DDoS attacks”, International Journal of Electrical and Computer Engineering (IJECE), Vol. 10, No. 2, April 2020, pp. 2182_2191.

[5] Azka Wani, S. Revathi, “Ransomware protection in loT using software defined networking”, International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 3, June 2020, pp. 3166~3175.

[6] H. Kim, J. Ko, D. E. Culler and J. Paek, "Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2502-2525, Fourthquarter 2017, doi: 10.1109/COMST.2017.2751617.

[7] A. M. Alberti, G. D. Scarpioni, V. J. Magalhães, A. Cerqueira S., J. J. P. C. Rodrigues and R. da Rosa Righi, "Advancing NovaGenesis Architecture Towards Future Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 215-229, Feb. 2019, doi: 10.1109/JIOT.2017.2723953.

[8] T. M. Fernández-Caramés, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6457-6480, July 2020, doi: 10.1109/JIOT.2019.2958788.

[9] N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[10] Bhavana A, “Evaluating Perception, Characteristics and Research Directions for Internet of Things (IoT): An Investigational Survey”, International Journal of Computer Applications (0975 – 8887) ,Volume 121 – No.4, July 2015.

[11] S. Yılmaz, E. Aydogan and S. Sen, "A Transfer Learning Approach for Securing Resource-Constrained IoT Devices," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4405-4418, 2021, doi: 10.1109/TIFS.2021.3096029.

[12] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang and K. -K. R. Choo, "An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security," in IEEE Transactions on Services Computing, vol. 13, no. 4, pp. 625-638, 1 July-Aug. 2020, doi: 10.1109/TSC.2020.2966970.

[13] K. Haseeb, N. Islam, A. Almogren and I. Ud Din, "Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things," in IEEE Access, vol. 7, pp. 185496-185505, 2019, doi: 10.1109/ACCESS.2019.2960633.

[14] T. Mick, R. Tourani and S. Misra, "LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 755-764, April 2018, doi: 10.1109/JIOT.2017.2725238.

[15] Y. Xu, J. Liu, Y. Shen, J. Liu, X. Jiang and T. Taleb, "Incentive Jamming-Based Secure Routing in Decentralized Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 3000-3013, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3025151.

[16] A. Raoof, A. Matrawy and C. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1582-1606, Secondquarter 2019, doi: 10.1109/COMST.2018.2885894.

[17] K. Haseeb, N. Islam, A. Almogren, I. Ud Din, H. N. Almajed and N. Guizani, "Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs," in IEEE Access, vol. 7, pp. 79980-79988, 2019, doi: 10.1109/ACCESS.2019.2922971.

[18] X. Guo, H. Lin, Z. Li and M. Peng, "Deep-Reinforcement-Learning-Based QoS-Aware Secure Routing for SDN-IoT," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6242-6251, July 2020, doi: 10.1109/JIOT.2019.2960033.

[19] A. Raoof, A. Matrawy and C. -H. Lung, "Enhancing Routing Security in IoT: Performance Evaluation of RPL’s Secure Mode Under Attacks," in

IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11536-11546, Dec. 2020, doi: 10.1109/JIOT.2020.3022276.

[20] D. Shin, K. Yun, J. Kim, P. V. Astillo, J. Kim and I. You, "A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks," in IEEE Access, vol. 7, pp. 142531-142550, 2019, doi: 10.1109/ACCESS.2019.2943929.

[21] I. Wadhaj, B. Ghaleb, C. Thomson, A. Al-Dubai and W. J. Buchanan, "Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL)," in IEEE Access, vol. 8, pp. 43665-43675, 2020, doi: 10.1109/ACCESS.2020.2977476.

[22] K. Saleem, G. M. Alabduljabbar, N. Alrowais, J. Al-Muhtadi, M. Imran and J. J. P. C. Rodrigues, "Bio-Inspired Network Security for 5G-Enabled IoT Applications," in IEEE Access, vol. 8, pp. 229152-229160, 2020, doi: 10.1109/ACCESS.2020.3046325.

[23] A. Ramos, R. T. P. Milfont, R. H. Filho and J. J. P. C. Rodrigues, "Enabling Online Quantitative Security Analysis in 6LoWPAN Networks," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5631-5638, June 2019, doi: 10.1109/JIOT.2019.2904302.

[24] Y. Liu, M. Ma, X. Liu, N. N. Xiong, A. Liu and Y. Zhu, "Design and Analysis of Probing Route to Defense Sink-Hole Attacks for Internet of Things Security," in IEEE Transactions on Network Science and Engineering, vol. 7, no. 1, pp. 356-372, 1 Jan.-March 2020, doi: 10.1109/TNSE.2018.2881152.

[25] Y. Sun et al., "Lightweight Anonymous Geometric Routing for Internet of Things," in IEEE Access, vol. 7, pp. 29754-29762, 2019, doi: 10.1109/ACCESS.2019.2902621.

[26] K. Haseeb, I. Ud Din, A. Almogren, N. Islam and A. Altameem, "RTS: A Robust and Trusted Scheme for IoT-Based Mobile Wireless Mesh Networks," in IEEE Access, vol. 8, pp. 68379-68390, 2020, doi: 10.1109/ACCESS.2020.2985851.

[27] R. H. Jhaveri, N. M. Patel, Y. Zhong and A. K. Sangaiah, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT," in IEEE Access, vol. 6, pp. 20085-20103, 2018, doi: 10.1109/ACCESS.2018.2822945.

[28] S. Sathyadevan, K. Achuthan, R. Doss and L. Pan, "Protean Authentication Scheme – A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments," in IEEE Access, vol. 7, pp. 92419-92435, 2019, doi: 10.1109/ACCESS.2019.2927818.

[29] P. Dass, S. Misra and C. Roy, "T-Safe: Trustworthy Service Provisioning for IoT-Based Intelligent Transport Systems," in IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 9509-9517, Sept. 2020, doi: 10.1109/TVT.2020.3004047.

[30] A. Agiollo, M. Conti, P. Kaliyar, T. -N. Lin and L. Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1178-1190, June 2021, doi: 10.1109/TNSM.2021.3075496.

[31] A. Bhavana, A. N. Nandha Kumar, "An Analytical Modeling for Leveraging Scalable Communication in IoT for Inter-Domain Routing", Springer-Proceedings of the Computational Methods in Systems and Software, pp.1-11, 2018.

[32] A. Bhavana, A. N. Nandha Kumar,"ICS: Interoperable Communication System for Inter-Domain Routing in Internet-of-Things", SAI-The Science and Information Organization, vol.10, Iss.5, 2021, 10.14569/IJACSA.2021.0120533.