International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Framework for Secure Routing Towards Identifying and Resisting Complex Malicious Threats in IoT Ecosystem

Ayasha M, Savitha Devi M

Abstract*: *Internet-of-Things (IoT) is an inevitable domain of technology that is going to capture the connectivity of the majority of the smart devices in the coming days supported by huge advancement in mobile computing. However, IoT still suffers serious security issues when it comes to performing extensive communication over a broad range of heterogeneous devices. A review of existing secure routing schemes shows that they are complex in operation overlooking the communication performance and resource-constrained factors. Therefore, the proposed system introduces a very novel, simple, and cost-effective, secure routing scheme that is not only capable of identifying the threats without any apriority information of adversary, but they are equally capable of isolating the threats from the connectivity of regular IoT nodes. The simulated outcome of the proposed system shows that it offers a better solution towards security in contrast to existing security approaches frequently exercised in IoT at present.

Keywords: Internet-of-Things, Security, Attack, Routing, Control message.

I. INTRODUCTION

There is an increasing proliferation of Internet-of-Things (IoT) in recent times owing to the progressive growth of mobile networks as well as mobile computing [1]. Basically, IoT can be briefed as a form of a global network that facilitates various systems to carry out either controlling or monitoring tasks by setting up a massive network of various devices [2]. Therefore, an IoT node can be considered to possess its sensing capability along with the capability to perform data transmission where specific event information is captured, processed, and forwarded by gateway node [3]. It will also mean that IoT consists of an amalgamation of heterogeneous network shrouded with various forms of security threats owing to its exposure to various networking protocols [4]. From the various routing schemes [5], IoT also offers various secure routing schemes, too [6]. Various forms of possible attacks in IoT are ranking based attack, sinkhole attack, hello flooding, wormhole attack, Denial-of-Service attack, neighbor attack, etc. [7]. Majority of the attacks targets to compromise the confidentiality, availability, and integrity factor in security, which always has an adverse effect over resource utilization, routing operation, and data processing mainly[8]. The existing security routing protocols are designed based on multihop routing [9], trust factor [10], acknowledge-based [11], group-based trust [12], collaborative trust [13], energy-aware trust [14], etc. However, all these secure routing schemes suffer from certain pitfalls. The first problem is related to the absence of standardization in secure communication while it also suffers from various computational complexity problems too. Another significant issue in the existing routing scheme is that resource constraints factors of the IoT nodes are not the part of considering while drafting secure routing schemes over the network layer. Apart from this, existing secured routing schemes in an IoT is also witnessed to use elementary procedures of security which is not enough for resisting complex forms of security threats in IoT. Problems still exist for setting up a secure routing scheme, stability factor of the routing scheme over the dynamic topology of mobile nodes, appropriate identification of the malicious node, the privacy of the location, etc. It is essential to know that secure routing protocols are very much crucial for error-free as well as resilience operation for the complete IoT environment. The most significant challenging factor associated with the existing secured routing scheme is to work out on a generalized security policy that can offer robust preventive measures against all forms of routing threats. The prime reason behind this is different adversaries bear specific attack launching strategy, and forecasting the nature of the severity of the attacker in upcoming communication is not feasible with respect to computational modeling. On the other hand, if there existing any form of a solution that can at least mitigate a maximum number of routing threats, then it will be somewhat possible to reduce the count of such attacks. Various forms of secure routing schemes have already been investigated e.g., trust management, encryption-based, and key management in an IoT environment. Therefore, the main motive of the proposed system is to evolve up with a completely novel solution that can not only perform intrusion detection but also perform intrusion prevention approaches. Section **"A"** discusses the existing literature where different security techniques towards offering resistivity in IoT have been presented, followed by a discussion of research problems in Section **"B"** and the proposed solution in **"C"**. Section **II** discusses about algorithm implementation followed by a discussion of result analysis in Section **III**. Finally, the conclusive remarks are provided in Section **IV.**

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Ayasha M*, Assistant Professor, Department of Computer Science, MGR College, Hosure, Dist- Krishnagiri, Tamilnadu, India.
Dr. Savitha Devi M, Assistant Professor & HoD, Department of Computer Science, Periyar University Constituent College of Arts & Science Harur, Dist- Dharmapuri, Tamilnadu, India

A. The Background

The Internet of Things (IoT) is gaining more attention and can be seen in various outdoor and indoor applications such as home, vehicles, and wearable devices. IoT includes a huge number of interconnected devices-(Things), which makes networking smarter and more sophisticated. With the increase in the number of IoT devices and applications, various security approaches have been introduced to make them more powerful and resilient against various attacks. The work carried out by Sathyadevan et al. [15] introduced lightweight authentication mechanism IoT end-devices where gateway plays as a role of an edge computing node. The work of Shin et al. [16] offered a route optimization scheme based on Distributed IP Mobility Management to offer a key exchange, interactive authentication, and privacy preservation. Yin et al. [17] presented SDx paradigm based architecture and designed a distributed denial-of-service attack detection algorithm using threshold value obtained from cosine similarity of the packet-in vectors at the boundary of presented architecture switch ports. In the study of Ding et al. [18], the authors have focused on cryptographic based edge computing and presented another technique to explore information about collision attack. Falco et al. [19] suggested an artificial intelligence-(AI) oriented cyber risks estimation strategies to secure smart cities against cyber attacks. Sairam et al. [20] introduced a Network Function Virtualization-(NFV) based security function using a network edge traffic pattern to provide enhanced security in the IoT ecosystem. The study of Choi et al. [21] has used ontology modeling to provide security services in power IoT-cloud ecosystem. Zhang et al. [22] relay-aided vectorized-(RAV) approach to provide secure data transmission and communication under the influence of pilot contamination attacks-(PCA) in IoT networks. Nguyen et al. [23] presented a review work on a complete power exhaustion attack in energy constraints wireless network. George et al. [24] suggested a graph-based security risk evaluation framework for the industrial IoT system. The work of Mangia et al. [25] presented an energy-efficient security technique based on Block-Chain mechanisms for energy constraints nodes in the IoT network. Das et al. [26] used EllipticCurve Cryptography and key-agreement techniques to design a lightweight security mechanism for the IoT system. Sharma et al. [27] utilize the approach of behavior rule specification to design a misbehavior recognition scheme for a cyber-based IoT ecosystem. Dynamic characteristics obtained from creeping wave propagation is utilized in the study Wang et al. [28] to provide safeguard to on-body IoT devices. The study of Hsu et al. [29] adopted trigger-action programming to describe the risk associated with security attacks and presented a hidden attack detection model. An efficient and robust data aggregation scheme is used in the work of Swathi and Yogish [30] for achieving data reliability in IoT. Bhandari and kirubanand [31] used a joint approach of symmetric-asymmetric encryption and Public Key Server to offer secure packet forwarding in IoT assisted applications. Similarly, the work of Oh and Lim [32] has presented an efficient routing protocol using the bloom filtering approach and improved rank concept. Tain et al. [33] have utilized the concept of Radio Frequency Fingerprint to resist Man-In-Middle-(MIM) security attack in industrial IoT. The study of Mangia et al. [34], discussed the effectiveness of compressed sensing for Low-cost security against known-plaintext attacks in IoT. The next section briefs about the problems associated with the existing security approaches in IoT.

B. The Research Problem

Significant research problems are as follows:

- Existing security solutions are mainly based on complex encryption or sophisticated process of assessing the threat whose viability is not assessed appropriately.
- The majority of the research-based solutions are quite specific to particular threats, and thereby, their applicability over the large network with exponential threat is questionable.
- Attacks begin from compromising the control message, which should be secured while there are no such attempts to secure such essential control messages.
- There is a need to perform an effective threat analysis over multiple levels without any overhead, which cannot be witnessed in the existing system.
- Therefore, the problem statement of the proposed study can be stated as "*Developing an effective and secure routing approach targeting to identify dynamic malicious patterns in any forms of threats to protect the resource-constrained IoT nodes is challenging task in routing operation*."

C. Proposed Solution

The core aim of the proposed study is to develop a novel security approach for securing the routing operation exercised in an IoT environment. An analytical research methodology has been used for constructing the proposed system where the prime emphasis is to introduce a non-conventional mechanism of intrusion detection and prevention system in the IoT environment considering the fact that this protocol should be executed over the resource constrained IoT devices. Figure 1 highlights the proposed research methodology.

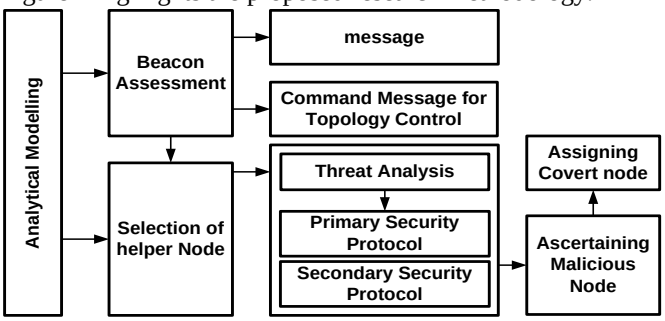

Fig.1 Proposed Research Methodology

As seen in Figure 1, it can be observed that there are two core modules involved in the entire design process viz. beacon assessment and selection of helper node. The study considers that devices are primarily wireless, and hence the majority of the threats are possible in the route discovery phases itself, and hence, beacons are required to be protected. The proposed system makes use of beacons which carry the messages (data packets) and command message for topology control. According to the logic introduced in the proposed system,

it is considered that such internal operations are hard to mimic and hence even if there are slighter chances that these messages are compromised, than the proposed system introduced a helper node which is also a normal IoT node responsible for forwarding the data packet and hence significant overhead for data dissemination can be resisted using this concept. The proposed system also introduces a unique threat analysis mechanism where two forms of progressive security protocols (primary and secondary) are constructed. This construction of the security protocol is meant for ensuring prevention of any form of malicious activity with an assumption that attackers are more greedy towards multiple links than compared to single links. Once the malicious nodes are ascertained, then the proposed system introduced a counterfeited node called a covert node, which is meant for broadcasting misleading routing information to the malicious node. Upon receiving the misleading route information, the malicious node expends its resources for the forged routes, and thereby, it drains its resources in this attempt. Hence, without using any cryptographic measures, the proposed sysem not only identifies attacker but also prevents them for any form of participation in routing.

II. SYSTEM IMPLEMENTATION

The proposed system is implemented considering all the practical situation of the malicious intention of an adversary in an IoT communication environment. In reality, the IoT environment consists of multiple heterogeneous numbers of the sensor, actuators, etc. that are highly interconnected with each other in order to form a group of a specific form of network. Applying a common and generalized security protocol will not solve the purpose, and therefore, the system implementation of the proposed study is carried out in such a way that it can resist the majority of attack just on the basis of their malicious intention behind every communication/routing based operation. This section discusses the assumptions being carried out, backbone implementation strategy, implementation design, and algorithm execution flow.

A. Assumption Carried Out

The primary assumption of the proposed study is that no attacker node will launch its malicious program instantly when they are introduced in the network of an IoT. This assumption will retain the practicality of attacker nodes as they will not possess predefined information of security policies already running in the network. The secondary assumption of the proposed system is that attackers are selfish in nature, and their profit of attack is defined by more number of multiple links that are compromised. This assumption will ensure the strength of the attacker to be higher and widespread that will assist in evaluating the effectiveness of the proposed security solution. The tertiary assumption of the proposed system is those gateway nodes are challenging to be compromised, and hence, the attacker will be more focused on attacking the normal IoT nodes. This assumption will offer the inclusion of vulnerable situations of a massive number of IoT devices that are more exposed to vulnerability as compared to the gateway node, which is always less in number.

B. Backbone Implementation Strategy

The complete design of the backbone strategy of proposed implementation is carried out on the basis of the existing routing strategies practices in the IoT environment, which is basically meant for controlling network overhead. The proposed system uses a similar mechanism with an inclusion of a specific relay node called as helper node, which is responsible for performing forwarding of the beacons over the entire network of an IoT. The selection of the helper node is carried out by an IoT node where the helper node will also permit the necessary coverage for all the dual links of the adjacent IoT nodes. The contents of the beacons forwarded by the helper node will consist of data as well as a command to control the network for altering the topology as on-demand. This is carried out in order to maintain better reliability of the data transmission process for a dynamic network. The hello message consists of information about the adjacent IoT nodes that are forwarded to all the IoT nodes whose response creates a single link between the responder node and source node in IoT. This finally results in the construction of local information associated with dual links that consist of all node connectivity information. All this information is retained securely in a gateway node. The protocol also demands all the IoT nodes to perform a periodic selection of the helper node by forwarding the command to control the network, and this process results in recording all the IoT nodes that have already performed a selection of the helper node. This phenomenon will be utilized for the identification of the malicious node as all the malicious node will attempt to compromise an IoT node that has connectivity with the helper node. Once the helper node is compromised, then the attacker node will have full control over the distributed topology of an IoT node inside the simulation area. Therefore, the idea of the proposed study is that if there is any node found to offer an illegitimate request to the IoT nodes (that can be now easily found by exploring the internal message information), then the helper node advertise about an imaginary node called as covert node with a forfeited address in order to attract the malicious user. This is an interesting idea of resisting the attacker as the attacker will think a covert node as a medium to make an entry to the complete network without even knowing that there is no such real node exists. The attacker node will spend all its resources in order to invoke attack over a network that doesn't exist at all while, on the other hand, the communication among the regular IoT nodes is continued.

C. Implementation Design

The complete implementation of the proposed system is based on the fact that it doesn't assess the validity of the message forwarded by the helper node, but it assesses the degree of integrity by exploring the ranges of contradiction between the alteration in the topology and messages. Figure 2 highlights the possible network situation of a proposed system where it can be seen that immediate neighboring nodes of 1 are 2, 5, and 8 that act as the formation of a single link, while the second layer of neighboring nodes of 1 is 3 and 6. Therefore, according to the proposed system, node-1 can choose the helper node as 2 and 5 in order to protect the second layer of neighboring nodes (i.e. 3 and 6).

Consider the presence of an attacker node 8 who seeks to launch malicious programs on 1. In such a case, node 8 will need to advertise a counterfeited message that could consist of routing information of neighboring nodes of 8 itself i.e., 1, 3, 6, and Cx (Cx is a covert node). However, the possibility of declaring 2 and 5 are very less as they are already a part of immediate neighbor nodes of 8, as in such case, node-1 can perform the assessment by distinguishing the message of the IoT node 8 with that of 2 and 5 respectively. Therefore, the *primary security protocol* developed for this situation is that when a message has been broadcasted by an attacker node 8 that consists of information related to immediate neighboring nodes of node 8 then the node 1 is supposed to offer a confirmation that the IoT nodes specified by node-8 are not a part of its immediate neighboring nodes of node 1 itself. This fact can be assessed by evaluating the prior message to find if they forwarded a confirmation to the source node as its neighboring IoT node.

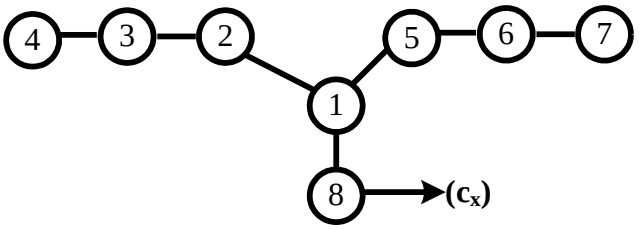

Fig.2 Possible Situation of IoT Node Compromization

The information of nodes 2 and 5 is anticipated to be present in the second layer of neighboring nodes of node 8, so node 8 must choose a helper node that permits to perform communication with such IoT nodes. However, there is all the possibility that node 8 can forge the fact that it chooses node as a helper node in order to protect nodes 2 and 5. In such a case, it will not be possible for node 1 to deny the request, and node 1 cannot confirm that if node 8 is malicious. On the other hand, it is feasible for node 1 to assess if node 8 has already selected other helper nodes for protecting the second layer of neighboring nodes of node 8 to node 2 and node 5, which is node 3 or node 6. Hence, the proposed system formulates *secondary security protocol* which states that node 1 should assess if there is a presence of any node which is an immediate neighboring node for target node in such a way that it is not declared in the message of source node as well as it also assesses if it is positioned at more than two links away from the target node 1. Once this conditional logic is met, the next condition will be to assess if the node 8 has selected immediate neighboring node as itself i.e., node-8 itself as the helper node for protecting itself. In order to offer more security, node 1 should consider a message consisting of all the immediate neighboring nodes of itself, and if found, than it should offer resistance through the covert node.

The adoptions of covert nodes are meant for resisting these types of problems. Consider that node 5 chooses a covert node C5 than the adversary node 8 will require selecting node 5 as its helper node. As this fact can be verified by the command message for altering the topology of node 5; therefore, there are fair chances that node 8 could get flagged as an adversary. Therefore, it will mean that if covert node C5 is considered, then it is feasible to ensure the presence of at least one IoT node that has non-inclusion of the message such that node 8 should select some helper node in order to protect it. However, if all the IoT node starts selecting a surplus covert node than there are possibilities of overhead too, which can be controlled by a threshold point. Apart from this, this problem of surplus covert nodes can be controlled by the following manner: all the IoT nodes will be considering adding a covert node such that their distance is less than 2 or 3 links. In such a manner, the attack can never proceed beyond the specific links. The covert node for node 1 should never match with an immediate neighboring node of node 1 itself. A newly introduced device should broadcast its covert node followed by the calculation of primary security rule. Finally, all the updating operations are carried out over a specific duration of time.The interesting point of the proposed implementation strategy is that it completely discourages any form of the intruder (it may be a malicious node or a *curious* regular node) by assessing the contents from the link matrix. Hence, the computation and management of the link matrix are highly important, and this mechanism doesn't even need to communicate or authenticate the same from gateway node, which means that it is highly cost-effective in its implementation over the real-world scenario. The next section briefs of the algorithm that is crafted to implement this proposed strategy of implementation.

D. Algorithm Execution Flow

In order to resist a regular IoT node for being exposed to malicious/compromised node or adversary in a dense IoT environment, the proposed algorithm basically aims for formulating a secure route planning which will facilitate the nodes to interact with only legitimate IoT nodes only. The proposed algorithm takes the input of *A* (area of deployment), *d* (density of IoT nodes), *N* (IoT nodes) that after processing yields an outcome of r_{table} (secured routing table). The steps of the routing table are as follows:

Algorithm for Secure Route Formation in IoT

Input: A(area of deployment), den (density of IoT nodes), N (IoT nodes)

Output: r_{table} (secured routing table)

Start

1. deploy rand(den)^A
2. $L_{mat} \rightarrow f_1((x,y), A, N)$
3. $H_{nodevec} \rightarrow f_2(N, L_{mat})$
4. $N_{cnode} \rightarrow f_3(N, c, rand)$
5. **For** i=1: length(x_c)
6. ix=explore(d<R)
7. coverage(i)→length(ix)
8. **End**
9. $[C_x\ C_y] \rightarrow [((x_c, y_f)(ix))]$
10. Establish connection (L_{mat}, (x,y), N)
11. $[r_{table}] \rightarrow f_4((x,y), N, L_{mat}, H_{nodevec})]$

End

The discussion of the steps of the algorithm is as follows: Initially, an IoT nodes N are randomly deployed over a simulation area of A considering specific node density of den (Line-1). Once the nodes are deployed, the next step is to formulate a link matrix L_{mat} on the basis of positional values (*x*, *y*) of an IoT node, area *A*, and a number of IoT nodes *N* (Line-2).

The complete link matrix is constructed considering the Euclidean distance between two IoT nodes where the neighbor nodes are decided on the basis of comparison of the distance between two nodes to be less than their respective transmission range R. This matrix also stores all the possible information of the single link and ensures that all the nodes are somehow connected to this single links. After the formation of the link matrix, the next step will be to determine helper node Hnodevec using an explicit function $f_2(x)$ that takes input of a number of IoT nodes *N* and link matrix newly constructed L_{mat} (Line-3). In order to determine helper node, the operation carried out by the respective function $f_2(x)$ are as follows: for all the IoT nodes N, the function extracts information of double links from the link matrix considering a set of two single links or node with two transmission vector found. The algorithm then finds the entire common single link and differentiates them from all the dual links adjacent IoT nodes. The intersection between two communication vector for single and dual links are extracted as *ix* matrix. The next task of the function is to explore the coverage where the single links with specific node identity are extracted, followed by exploring the common nodes with dual links followed by sorting in order to generate a communication vector. This operation is also followed obtaining the identity of the adjacent IoT nodes along with exploring the IoT nodes with better coverage giving a yield of helper node vector or $H_{nodevec}$ (Line-3). After the construction of the helper node vector is over, all the non-repeating $H_{nodevec}$ are extracted, followed by the value of it. The next operation is to deploy covert IoT nodes as the prominent shield of security using another explicit function $f_3(x)$ considering the input of IoT nodes *N*, network constant *c* that generates a number of covert nodes required to be deployed as a matter of prevention (Line-4). For all the position of the covert nodes (x_c, y_c) (Line-5), the proposed algorithm randomly deploy covert nodes considering the distance *d* between covert nodes and target node (relay node under attack). Only the distance *d* lesser than transmission range *R* is stored in *ix* matrix (Line-6) followed by determining the coverage on the basis of length of this *ix* matrix (Line-7). The algorithm then obtains the highest possibility of the coverage IoT node as a covert node. The algorithm than formulates forged matrix which, keeps on evolving involuntarily on the basis of attack intensity [C_x C_y], and this formulation is carried out over the index of the covered IoT node (Line-9). It will mean that it will be carried out by eliminating the target node, and thereby it protects disclosing the identity of the vulnerable node. This operation is followed up by establishing a communication connection between the next regular IoT nodes (Line-10) followed by updating of routing table rtable (Line-11), and this information is finally updated to all the other IoT nodes that are now reachable to all information about the regular IoT nodes in an IoT environment. The next section discusses about the results being obtained from the proposed system implementation.

III. RESULT ANALYSIS

The scripting of the proposed study has been carried out in MATLAB, considering 50-100 IoT nodes spread randomly across 1100x1300m2 simulation areas. The assessment of the proposed system is carried out considering unique performance parameters i.e., size of average message and percentage of required helper nodes. The prime reason behind this is if the size of the average message is found to be degraded, then the presence of an attacker is still there, whereas the percentage of required helper nodes are required to be diminished. Apart from this, the outcomes are compared with the existing approach of Chze and Leong [35] that is found to be standard multi-hop routing in IoT

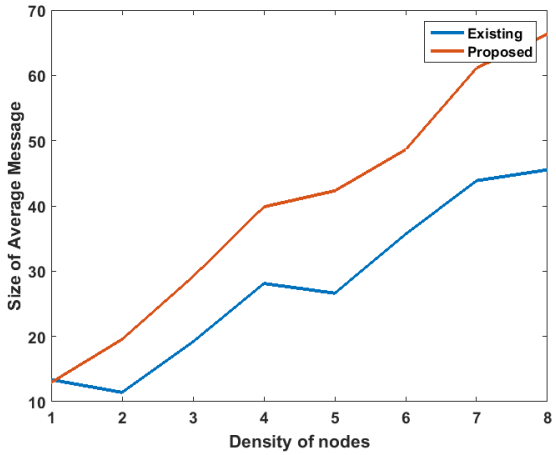

Fig.3 Comparative Analysis of Size of Average Message

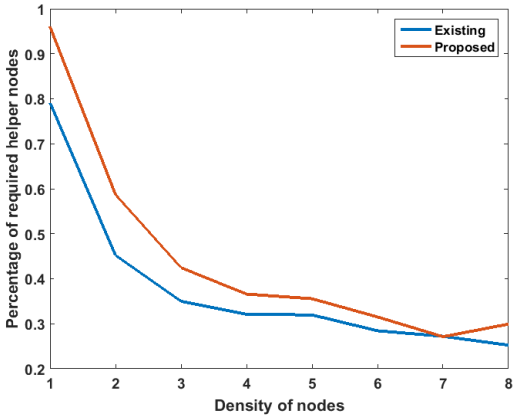

Fig.4 Comparative Analysis of Helper Node Dependencies

A closer look into figure 3 and figure 4 shows that the proposed system offers lower overhead and higher security as compared to the existing approach. Much overhead is created due to the adoption of a multihop based authentication mechanism in the existing system, whereas the proposed system offers formation of link matrix where only the single formed links are considered for route establishment. Apart from this, an increase in node density is also found to offer better throughput, as seen in figure 3, while overhead is significantly controlled, as seen in figure 4, where the proposed system can continue offering robust security with a reduction in dependencies over helper node.

IV. CONCLUSION

This paper has presented a novel secure communication approach towards safeguarding data transmission among IoT devices. The significant contribution of the proposed system are as follows:

i) the proposed system has not used conventional security mechanism e.g., trust, reputation, encryption, key management, etc. but yet it can offer similar resiliency in IoT routing operation, ii) the proposed system has introduced the concept of helper node and covert node without adding any form of external resources to facilitate an adequate security strength, iii) the secure routing scheme is first of its kind where both identification and prevention strategy is formulated in IoT, iv) the complete mechanism of identification of threats doesn't have any dependency toward predefined information of threats. Our future work will be continued to further improve resiliency by using optimization schemes.

REFERENCES

1. Aljarah, Maha, Mohammad Shurman, and Sharhabeel H. Alnabelsi. "Cooperative-Hierarchical Based Edge-Computing Approach for Resources Allocation of Distributed Mobile and IoT Applications." International Journal of Electrical and Computer Engineering (IJECE) 9, no. 1 (2019).
2. Da Xu, Li, Wu He, and Shancang Li. "Internet of things in industries: A survey." IEEE Transactions on industrial informatics 10, no. 4 (2014): 2233-2243.
3. Zhu, Qian, Ruicong Wang, Qi Chen, Yan Liu, and Weijun Qin. "Iot gateway: Bridgingwireless sensor networks into internet of things." In 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp. 347-352. Ieee, 2010.
4. Zhao, Kai, and Lina Ge. "A survey on the internet of things security." In 2013 Ninth international conference on computational intelligence and security, pp. 663-667. IEEE, 2013.
5. Zhao, Kai, and Lina Ge. "A survey on the internet of things security." In 2013 Ninth international conference on computational intelligence and security, pp. 663-667. IEEE, 2013.
6. Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "Secure routing for internet of things: A survey." Journal of Network and Computer Applications 66 (2016): 198-213.
7. Rghioui, Anass, Anass Khannous, and Mohammed Bouhorma. "Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition." Journal of Advanced Computer Science & Technology 3, no. 2 (2014): 143.
8. Oteafy, S., and Hossam S. Hassanein. "Resource re-use in wireless sensor networks: Realizing a synergetic internet of things." Journal of Communications 7, no. 7 (2012): 484-493.
9. Chze, Paul Loh Ruen, and Kan Siew Leong. "A secure multi-hop routing for IoT communication." In 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 428-432. IEEE, 2014.
10. Mahmud, Mufti, M. Shamim Kaiser, M. Mostafizur Rahman, M. Arifur Rahman, Antesar Shabut, Shamim Al-Mamun, and Amir Hussain. "A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications." Cognitive Computation 10, no. 5 (2018): 864-873.
11. Nepomuceno, Joven Daniel R., and Nestor Michael C. Tiglao. "Performance evaluation of 6TiSCH for resilient data transport in wireless sensor networks." In 2017 International Conference on Information Networking (ICOIN), pp. 552-557. IEEE, 2017.
12. Kamble, Arvind, Virendra S. Malemath, and Deepika Patil. "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey." In 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), pp. 33-39. IEEE, 2017.
13. Wen, Bin, Ziqiang Luo, and Yazhi Wen. "Evidence and Trust: IoT Collaborative Security Mechanism." In 2018 Eighth International Conference on Information Science and Technology (ICIST), pp. 98-9. IEEE, 2018.
14. Duan, Junqi, Deyun Gao, Dong Yang, Chuan Heng Foh, and Hsiao-Hwa Chen. "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications." IEEE Internet of Things Journal 1, no. 1 (2014): 58-69.
15. Sathyadevan, S., Achuthan, K., Doss, R., & Pan, L. (2019). Protean Authentication Scheme–A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments. IEEE access, 7, 92419-92435.
16. Shin, D., Yun, K., Kim, J., Astillo, P. V., Kim, J. N., & You, I. (2019). A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks. IEEE Access, 7, 142531-142550.
17. Yin, D., Zhang, L., & Yang, K. (2018). A DDoS attack detection and mitigation with software-defined Internet of Things framework. IEEE Access, 6, 24694-24705.
18. Ding, Y., Shi, Y., Wang, A., Zheng, X., Wang, Z., & Zhang, G. (2019). Adaptive Chosen-Plaintext Collision Attack on Masked AES in Edge Computing. IEEE Access, 7, 63217-63229.
19. Falco, G., Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A master attack methodology for an ai-based automated attack planner for smart cities. IEEE Access, 6, 48360-48373.
20. Sairam, R., Bhunia, S. S., Thangavelu, V., & Gurusamy, M. (2019). NETRA: Enhancing IoT Security using NFV-based Edge Traffic Analysis. IEEE Sensors Journal, 19(12), 4660-4671.
21. Choi, C., & Choi, J. (2019). Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service. IEEE Access, 7, 110510-110517.
22. Zhang, N., Wu, R., Yuan, S., Yuan, C., & Chen, D. (2019). RAV: Relay Aided Vectorized Secure Transmission in Physical Layer Security for Internet of Things Under Active Attacks. IEEE Internet of Things Journal.
23. Nguyen, V. L., Lin, P. C., & Hwang, R. H. (2019). Energy Depletion Attacks in Low Power Wireless Networks. IEEE Access, 7, 51915-51932.
24. George, G., & Thampi, S. M. (2018). A graph-based security framework for securing industrial IoT networks from vulnerability exploitations. IEEE Access, 6, 43586-43601.
25. Mangia, M., Marchioni, A., Pareschi, F., Rovatti, R., & Setti, G. (2019). Chained Compressed Sensing: A Block-Chain-inspired Approach for Low-cost Security in IoT Sensing. IEEE Internet of Things Journal..
26. Das, A. K., Wazid, M., Yannam, A. R., Rodrigues, J. J., & Park, Y. (2019). Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment. IEEE Access, 7, 55382-55397.
27. Sharma, V., You, I., Chen, R., & Cho, J. H. (2019). BRIoT: Behavior Rule Specification-based Misbehavior Detection for IoT-Embedded Cyber-Physical Systems. IEEE Access.
28. Wang, W., Yang, L., Zhang, Q., & Jiang, T. (2018). Securing on-body IoT devices by exploiting creeping wave propagation. IEEE Journal on Selected Areas in Communications, 36(4), 696-703.
29. Hsu, K. H., Chiang, Y. H., & Hsiao, H. C. (2019). SafeChain: Securing Trigger-Action Programming from Attack Chains. IEEE Transactions on Information Forensics and Security.
30. Swathi, S., & Yogish, H. K. (2019). Secure data aggregation in IoT using efficient-CSDA. International Journal of Electrical & Computer Engineering (IJECE) (2088-8708), 9.
31. Bhandari, R. (2019). Enhanced encryption technique for secure iot data transmission. International Journal of Electrical & Computer Engineering (2088-8708), 9.
32. Oh, H., & Lim, S. (2016). Light-weight Routing Protocol in IoT-based Inter-Device Telecommunication Wireless Environment. International Journal of Electrical and Computer Engineering (IJECE), 6(5), 2352..
33. Tian, Q., Lin, Y., Guo, X., Wen, J., Fang, Y., Rodriguez, J., & Mumtaz, S. (2019). New Security Mechanisms of High-Reliability IoT Communication Based on Radio Frequency Fingerprint. IEEE Internet of Things Journal.
34. Mangia, M., Pareschi, F., Rovatti, R., & Setti, G. (2017). Low-cost security of iot sensor nodes with rakeness-based compressed sensing: Statistical and known-plaintext attacks. IEEE Transactions on Information Forensics and Security, 13(2), 327-340.

Chze, Paul Loh Ruen, and Kan Siew Leong. "A secure multi-hop routing for IoT communication." In 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 428-432. IEEE, 2014.

AUTHOR'S BIBILIOGRAPHY

Ayasha M pursuing her **Ph.D(cs)** in Periyar University, Salem. She did her **M.C.A** from Bangalore university and **M.Phil** from Periyar University, Salem. She completed her under graduate course in Al-Ameen Arts College, Bangalore, India. She is currently working as an Assistant Professor, Department of Computer Science, MGR College, Hosur, Krishnagiri Dist, Tamilnadu, India

Dr. Savitha Devi M completed her **Ph.D** in Mother Teresa Women's University, Kodaikanal. She done her **M.C.A** and **M.Phil** from Periyar University, Salem, and studied her **M.Sc** Computer Science in Vysya College, Salem where she got University 11th rank in the year 2003. She completed her under graduate course in Government Arts College, Salem. She began her carrier as Assistant Professor in Computer Science in **AVS College**, Salem in 2003. Then she joined in **Don Bosco** College, Dharmapuri as a **Faculty, Head of Department, Research coordinator** as well as member in various committees. Currently she is working as an Assistant Processor and Head in Computer Science, Periyar University Constituent College of Arts and Science, Harur-636903, Dharmapuri District, TamilNadu, and continuing her admirable job in the 16th year.