International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 4, August 2020, pp. 3451~3459
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i4.pp3451-3459

Tactical approach to identify and quarantine spurious node participation request in sensory application

Somu Parande, Jayashree D. Mallapur
Department of Electronics and Communication, Basaveshwar Engineering College, India

Article Info

Article history:

Received Sep 6, 2018
Revised Jan 27, 2020
Accepted Feb 8, 2020

Keywords:

Attacks
Energy
Security
Spurios message
Wireless sensor network

ABSTRACT

Securing Wireless Sensor Network (WSN) from variable forms of adversary is still an open end challenge. Review of diversified security apprroaches towards such problems that they are highly symptomatic with respect to resiliency strength against attack. Therefore, the proposed system highlights a novel and effective solution that is capable of identify the spurios request for participating in teh network building process from attacker and in return could deviate the route of attacker to some virtual nodes and links. A simple trust based mechanism is constructed for validating the legitimacy of such request generated from adversary node. The proposed system not only presents a security solution but also assists in enhancing the routing process significantly. The simulated outcome of the study shows that proposed system offers significantly good energy conservation, satisfactory data forwarding performance, reduced processing time in contrast to existing standard security practices.

Corresponding Author:

Somu Parande,
Department of Electronics and Communication,
Basaveshwar Engineering College,
Bagalkot, Karnataka, India.
Email: somuparande63@gmail.com

1. INTRODUCTION

The wireless sensor network (WSN) is developed by MEMS together with communication and network systems. Previously, the WSN application started with small scale industry, next it is employed to the large scale real-time application [1]. The WSN is the combination of various and different sensor nodes which sense the data and collect the information based on the application requirement from the nearby atmosphere then gathered collected data to its data center through a radio-link medium [2]. WSN utilizes different types of sensors for sensing event such as temperature sensor, humidity sensor, pressure sensor, sound sensor (Ultrasonic), air sensor, proximity sensor etc. are participats to senses the sorrounding information [3]. The sensor, actuator, and computation nodes are the main compontents of the WSN [4]. There are different types of WSN that observed for deploying in many areas such as terrestrial WSN, under ground WSN, under water WSN, multimedia WSN, mobile WSN [5]. The WSN are highly installed for many critical and emergence applications such as aireborne, smart military, health monitoring, industrial process control, security and servilence, habitate monitoring, fire in forest, smart road and smart building, etc. The WSN technology is more essential for deploying a sensor node in harsh or hostile area where the wired connection and human interation is not able to organize their specific task such as forest, under ground, and under water etc. The WSN system is scalable and flexible which is the major advantage and has some disadvantages that are limited in sensing range, low storage capacity and less power storage capability [6].

The prime challenge of the WSN is dense sensor node deployement, limited energy capacity, sensor location, limited hardware resources, random deployment, data aggregation, scalability. Hence, the various limitation of WSN requires different security challenges to tackle such constraint problems. Big efforts are

applied by many researchers to overcome the security issues in WSN and other constraints of WSN [7-8]. Also, many security protocols are suggested by the researchers and practicioner such as cryptography, secure routing, and keymanagement scheme and etc [9-10]. Therefore, the proposed paper presents a completely new security approach that uses non-conventional approach in order to address threats from majority of the attacks in WSN and imposes cost effective solution with better performance in WSN. Section 1 (a-c) discusses about the existing literatures where different techniques are discussed for detection schemes used in power transmission lines followed by discussion of research problems and proposed solution. Section 2 discusses about algorithm implementation followed by discussion of result analysis in Section 3. Finally, the conclusive remarks are provided in Section 4.

a. The background

This section discusses the previous research work on security, privacy in WSN and network protocols. The work carried out by Ying Liu [11] have uses S-dLMS (Secure diffution Mean Square) Algorithm for security over distributed network against various attacks. Tayebi et al. [12] presents a chaotic DS-SS (Direct Sequence Spread Spectrum) method for improving the security in WSN. Luo et al. [13], introduced a well-organized Access Control system for security in the cross domain setting of internet of things. Illiano et al. [14] introduce an Anomal detection scheme with optimization algorithm for WSN event integrity. Hajji et al. [15], presents an efficient multi routing protocol for maximizing the lifetime of the WSN by increasing the critical node life. Sun et al. [16], adapts an intrusion detector model based on V- detector scheme for detection of interference in WSN. Zhang et al. [17], introduces an anonymous key exchange protocol based on the cryptographic technique (ECC) for addressing security and privacy measures. Kumar et al. [18], addressed a localization algorithm to secure the sensor node attacks and detection of malicious anchor node of privileged the network. Li et al. [19], adapts a DV (Distance Vector) hop algorithm which based on vector routing that offers security against wormhole attacks. Umar et al. [20], presents a trust based cross layer framework (TruFix) using trust based fuzzy mechanism for security against different types of attacks in WSN. Guan and Ge [21], addressing the distributed network security in WSN against jamming attacks with the help of markov jump model. Shen et al. [22], presents an ID (Identity) based comprehensive signature system for the protection of data integrity in WSN and also for reducing the bandwidth. Zhang et al. [23], introduces an interference detection based on trust mechanism and state context for resoiurce overhead and malicious identification in WSN. Rana [24], adapts a convex state approximation (CSA) algorithm for smart vehilcle cyber attacks. Nurellari and McLernon [25], presents a distributed detection system using optimum fusion rule for mitigating the security against attacks in WSN. Shafiee [26], discusses a different comparative method with spectrum sensing (SS) algorithm in cognitive WSN for the usage next generation WSN. Liu and Dong et al. [27], adapts an active trust system for trustable, efficirnt and secure routing in WSN which improves the data security. Mehmood et al. [28], introduces a knowledge based CAS (Context Aware Scheme) for identifying the attacks and dealing the interruption occur in the malicious node. Li et al. [29], introduces an authentication or security protocol for privacy protection of internet of things (Industrial feild) using optimal technique. Prasanta Gope [30], presents an authentication protocol for security in data acces in real time environment using cryptographic techniques.

Faisal et al. [31] have created a novel scheme based on receive signal strength mechanism to counter the identity replication attack on the IEEE 802.11 based wireless ad-hoc network. The study of Tayebi et al. [32] have presented improved chaotic based direct sequence spread spectrum (DSSS) technique in order to enhance the security of chaotic-DSSS dependent WSN. Tian et al. [33] have presented a modified version of mixed integer and nonlinear programming and gave a joint approach of full duplex and security by considering cross-layer optimization to improve the energy utilization, spectrum efficiency and to enhance the security level. The work of Hajji et al. [34] have introduced a novel multiobjective secure routing protocol for optimizing overall network resource in order to get quality aware data processing, network reliability and maximum life-span of WSN. Alshinina et al. [35] offers an advanced approach based on deep learning technique to provide a secure interface between end-user and WSN. The experimental effects display that it allows for secure data transmission from WSN to end-user with utilizing optimum network resources.

Kumar et al. [36] focused on the issue related with secure localization of sensor nodes and presented a secure localization algorithm to protect the sensor nodes from the outsider attack and as well as it also monitors the insider node to detect compromised node in the network. Luo et al. [37] have presented a secure and robust Access control design based on certificate-less and id-based cryptography technique for WSN in the cross Domian framework of IoT. Guan and Ge [38] have designed Markov chain and level switching based secure model to perform a safe estimation operation under a jamming attack.

b. The research problem

The significant research problems are as follows:

- Existing approaches are bit inclined towards using encryption techniques that is either mathematically complex or is iterative in its operation.
- The degree of spruriousness in the control messages are not offered much importance in the existing approaches causing massive fatalities in the network breach.
- The existing mechanism of trust computation demands updated information which is a bigger challenge for large scale network.
- Emphasis on practicality as well as computational complexity over processing time is something that is not much found in existing system.

Therefore, the problem statement of the proposed study can be stated as "*It is quite a difficult task to offer simple and potential security solutions to resist lethal threats in WSN using cost effective computational approach*". The next section discusses about the proposed system to address this problem.

c. The proposed solution

In order to ensure better robustness towards majority of the security threats, it is essential to identify the degree of legitimacy of the traffic system. As there are various forms of nodes joins and leaves the network, it is essential to develop a dynamic trust system. The core ideology of the proposed study is to evolve up with a simple and progressive strategy to capture all forms of request generated by the adversary as the first step to stop intrusion over WSN. Adopting analytical research methodology, the proposed system presents a simple scheme shown in Figure 1.

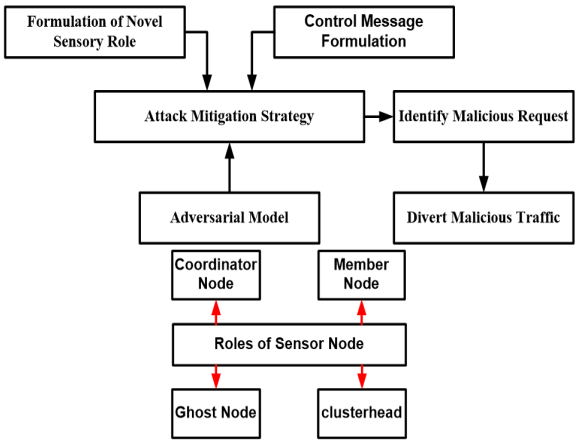

Figure 1. Analytical scheme of proposed methodology

The proposed system introduces a novel coordinator node system that is meant for minimizing the network overhead by assisting in enhancing the data transmission rate. Basically, coordinator node is a special responsibility of a clusterhead that finally takes a decision of finally forwarding the data packet to the neighboring node or to the sink.It also takes a decision of many other essential operations and hence its capabilities can be used maliciously by the adversary. Hence, it is essential that coordinator node should be elected and that rights are retained only within the currently operational clusterhead. The control message has been worked upon to split the operation of route request for bearing the specific information associated with updates using routing matrix. A new adversarial model has been introduced by generalizing majority of the lethal threats in WSN who are more targeting to attack network with higher links and connectivity. The proposed system introduces a mechanism where the malicious request is identified and then diverted into different direction thereby wasting resources of the adversarial node. The significant contribution of the proposed solution is that it offers capability to stop the intrusion in its first attempt itself. The next section elaborates about the system design.

2. ALGORITHM IMPLEMENTATION

This section offers illustration to the algorithm implemented for the purpose of resisting spurious network participation request. The design of the proposed algorithm is based on the agenda that any form of request that is directed to the clusterhead must be subjected to assessment for any form of security breach.

However, this is absolutely not an easy task and hence the proposed system introduces a new secure communication scheme for addressing this problem. The proposed system introduces three distinct algorithms that is responsible for incorporating security as discussed below:

2.1. Algorithm for trust computation

The proposed system constructs a memory in the form of routing table that retains all the successful occurance of routes most recently as well as in the start of current data aggregation in WSN. This table is called as trust table and it occupies only 5% of memory consumption irrespective of any size of network as it only stores information of set of nodes that has prior history of successful delivery of data. The steps involved in the algorithm are as follow:

Algorithm for trust computation
Input: p, n, T_x
Output: t_{value}
Start
1. init p, n, T_x
2. For i=1: n
3. $p_1 \leftarrow p$
4. $d \rightarrow ED(p, p_1)$
5. If ($d>0$ && $d \leq T_x$)
6. $t_{table}(i)=1$
7. End
8. End
9. For j=1: n-1
10. $sh \rightarrow find(t_{table}(j)==1)$
11.End
12. $t_{value}=[f(sh, t_{table})]$
End

This algorithm takes the input of p (position of sensor), n (node population), and T_x (transmission range) which after processing leads to t_{value} (trust value). The algorithm considers all the sensors (Line-2) and obtains the information of positions (p and p_1) of any two communicating sensors (Line-3 and Line-3). The trust table is built only for the communicating nodes and its associated neighboring nodes (condition highlighted in Line-5). A binarized mechanism of allocating the trust of the node is carried out. It should be known that such trust computation is carried out by any forms of sensors (clusterhead and member node). The next task is to obtain the information associated with the node that holds single hop *sh* neighboring nodes only (Line-10). Although, the source node is linked with all the forms of node that is connected with both single and multihop networks, but only the single hop information is retained within the trust table. This operation has two benefits i.e. i) consumption of lower memory and ii) heuristic information of only positive trust retained by sensors. An explicit function $f(x)$ is used for taking the inputs from single hop *sh* and all connected trust table t_{table} of other neighboring nodes in order to formulate final trust

2.2. Algorithm for constructing coordinator node list

A coordinator is a special form of sensory role where some of the best clusterheads are selected in order to perform two operations i.e. i) makes a decision to perform packet forwarding to the selected clusterhead in its vicinity or sink in vicinity and ii) implements a decision of topological changes when demanded after every cycle of data aggregation. Therefore, this algorithm maintains a list of all the selected clusterhead that will be acting as coordinator node and hence they attract the attention of adversary node who wants to gain an illegitimate access in order to experience the priviledge of coordinator node. The prime concept of building this algorithm is that an adversary node will be more interested in invoking maximum attack and for this they will be more *curious* about nodes with connected multihop network whereas proposed algorithm will restrict itself to only single hop. That will mean that for any request of network participation, coordinator node will offer access to a node using single hop only. The benefit of this idea is that even if the request is found to be malicious afterwards it will inflict its damage over single node and not on complete network and there by 98% of the network is protected. The significant steps of the algorithm are as follows:

The algorithm takes the input of n (sensor node) and t_{value} (trust value). The algorithm considers all the sensors and extracts information of all the sensors information retained with the memory of ttable in order o look for multi-hops (Line-2). A multi-hop matrix *mh* is formed where m=2, 3, 4….This operation is further followed by exploring single hop links that are found within multihop matrix (Line-4). This operation links

almost all the nodes and assists in offering much better accessibility while performing routing. In order to resists forming any form of redundant data, the algorithm extracts only unique information of the both single and multi hop nodes (Line-7). The proposed system also determine the strength of the coverage of both single and multihop nodes that is further sorted (Line-10).One interesting fact to be seen in this algorithm construction is that it is all about retention and accessibility of single and multihop routes so that when demanded it can offer accessibility as well as retriction too. Accessibility is offered by giving neighboring information of single hop and restriction is maintained by not furnishing any information of multihop network to new node n_{new}.

Algorithm for constructing coordinator node list
Input: n (node population),
Output: c_{node} (coordinator node list)
Start
1. For i=1:n
2. mh→find(t_{value}(i)==m)
3. For j=1:length(mh)
4. ix_2→unique[find(t_{value}(j) = =1)]
5. For k=1:length(ix)
6. h_{id}→find(t_{value}(k)==1)
7. cov→length(inter(h_2, h_1)
8. End
9. End
10. c_{node}→sort(cov)
11.End
End

2.3. Algorithm for identifying and isolating attacker

This algorithm is responsible for identifying and isolating the adversary from the entire network. The algorithm introduces a ghost node that performs diversion of the spurious request originated from the attacker node. The algorithm takes the input of r_{req} (route request) that after processing leads to the identification of the type of the newly participating sensor nodes. The significant steps of the proposed system are as shown below:

Algorithm for identifying and isolating attacker
Input: r_{req} (route request)
Output: type(n_{new})
Start
1. n_{new}→broadcast(r_{req})
2..For all r_{req} (n_{new})
3. If r_{req}(n_{new})≤1-hop
4. add r_{req}→temp
5. If r_{req}(t_{value})~cum(t_{value})
6. temp→new entry in t_{table}
7. Else if
8. Forward request to g_{node}
9. g_{node}→r_{rep} (fake_routes)
10. End
11. declare type(n_{new})→malicious
12. Update t_{value} & t_{table}
13. End
End

The attack mitigation strategy of the proposed system is very unique. The first level of protection involves formulating a routing table that retains information of diversified hops for active connections only. After receiving the malicious request of an adversary, the source node compares it with that of local updates, which will never match. In such case, the source node appoints a non-existing node using IP masking called as primary ghost node who forwards a fake profiles of IP of node that never exists in the existing network. As the primary ghost node forwards information in such a way that adversary believes the information forwarded by ghost node and allocates its resources to achieve it in second level of protection. In third level of protection, the adversary makes communication with secondary ghost node that is again virtually

developed by primary ghost node. One interesting point to be observed is that proposed system doesn't implement any form of encryption mechanism and it performs simple heuristic-based comparisons to find if the incoming request is legitimate or not. In case it is found illegitimate than it appoints a non-existing set of nodes that is means for generating a confusive and non-existing network that leads to degradation of resources by the attacker and thereby discourage them from any further attacks.

The algorithm initiates with the broadcasting operation of route request (r_{req}) of the new node n_{node} in order to participate in the network (Line-1). At this point, it is yet not known if n_{node} is genuine node or malicious node. If the request generated by the n_{new} is found to be looking for single-hop (Line-3) than the source node allows an access only to its single hop neighboring nodes provided if the trust value of the n_{new} is equal to that maintain in t_{table}. Otherwise, it doesn't give the access. However, if the request type of the n_{new} is found not to be matching with that of t_{table} (Line-7) than it is considered as a malicious node and soon that request is forwarded to the ghost node g_{node} which then constructs fake nodes as well as fake routes and allocate them as a route response rrep to the malicious node (Line-11). The malicious node has no other option than choosing that route request that cost them unwanted resources. Majority of the existing routing scheme in WSN uses only four types of control message i.e. route_request, route_reply, route_acknowledgement, and route_error. However, the proposed system makes slight changes in route_reply by forwarding the reply of controlling the node's action as consequences of data aggregation. The route_request message performs declaration of the information related to neighboring nodes of a target node. The severity of the attack is judged by the intrusion level over the route_request control message. The broadcasting of the route_reply is carried out by coordinator node periodically and such messages are only forwarded via coordinator node thereby minimizing the overhead. It was seen from the existing approaches that they are highly specific to a single form of attack which renders inapplicability of the existing approaches. Therefore, a new adversarial model is designed in such a way that it incorporates malicious behaviour of majority of the lethal threats in WSN. In this process, the vulnerable node will try to perform less broadcasting in order to ensure that they are not much exposing their location and resources to too many of the sensors. The attacker node, on the other hand, will try to extract more information from such vulnerable node in order to obtain information of large chain of networks which exists in multihop. For this purpose, the attacker node broadcast a falsified control message of route_request just to show that they are available to act as a coordinator node for the target source node. It is because once they become coordinator node than they will gain rights to use route_reply and start controlling the topology maliciously. Figure 2 presents a schemes to divert malicious node.

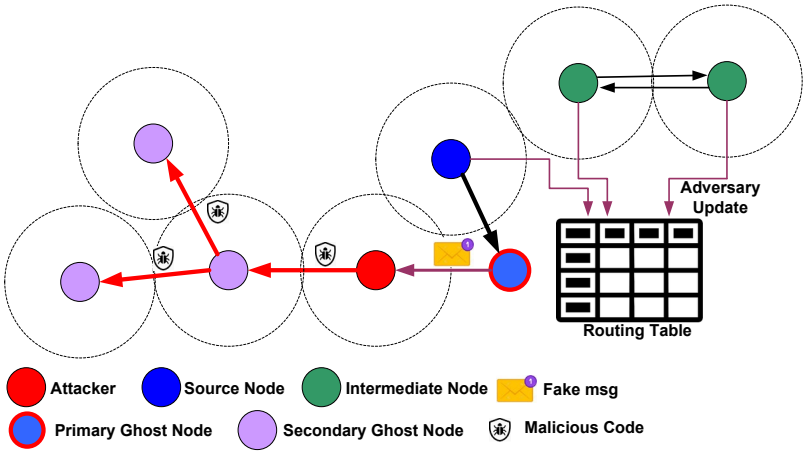

Figure 2. Schemes to divert malicious node

3. RESULT ANALYSIS

This section outlines about the simulation outcomes carried out in the proposed research work. In order to assess the performance of the proposed system, it is essential to understand that proposed study introduces a novel mitigation strategy for security. It is necessary to ensure that security performance should be ensured not at the cost of data delivery performance. Therefore, the analysis of security approach is carried out using some practical parameters e.g. residual energy and throughput. The simulation has been carried out considering 500-600 sensors bearing MicaZ mote property randomly spread over 1000x1100 m^2 simulation area. Analysis of dependency of ghost node is shown in Figure 3.

Figure 3 shows that there is a reduced dependency of Ghost node to divert the traffic with increase of node density. Reduction in the percentage of the ghost node also means that there is a reduction in an event of adversaries. The prime reason behind the reduction of the ghost node is that with the increasing event of complying with the falsified traffic generated by the ghost node, the attacker waste lots of resources in a process of performing routing. At the same time, this information of identified rogue nodes are periodically updated in the routing table which is also accessible by frequently newly joined nodes. This progressively minimizes need of the ghost node within the traffic system. Minimization of ghost node will also means reduction of spurios traffic system. Comparative analysis of residual energy. Comparative analysis of residual energy is shown in Figure 4.

The outcome shows that proposed system offers better energy retention capability as well as better form of data delivery services as shown in Figure 5. As SecLEACH [39] carry out random key distribution; hence it undergoes multiple checks just to authenticate the malicious request. Similarly, S-LEACH [40] speed up this process using pairwise key distribution, however, when the attacks are dynamic, S-LEACH slowly drains energy. For similar reason, performance of throughput is affected by existing approaches. Although, they are claimed to be preventive against various threats, such prevention cost is more than performance anticipated for existing system. The proposed system uses highly progressive approach of confirming the legitimacy of incoming request to understand the threat level and uses coordinator node which reduces lot of work load during data aggregation.

From Figure 6, it can be seen that proposed system offers highly reduced processing time as compared to existing S-LEACH and SecLEACH with increasing simulation rounds. The prime reason behind this is propose system offers increasing number of alterative which ensures faster secured route selection process along with better resistivity while existing approaches uses encryption-based mechanism where level of encryption fluctuates with increasing node over simulation trials.Hence, proposed system consumes 0.223 seconds while existing system consumes 1.75 seconds approximately for processing.

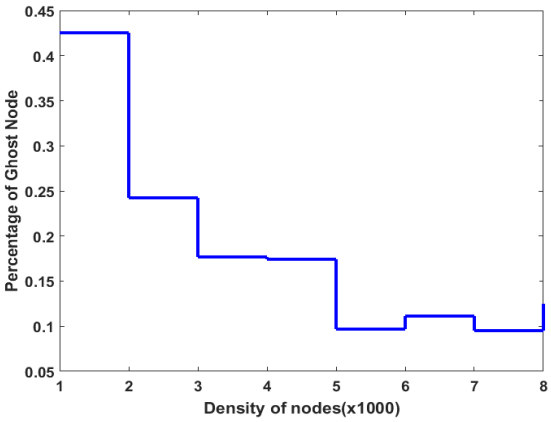

Figure 3. Analysis of dependency of ghost node

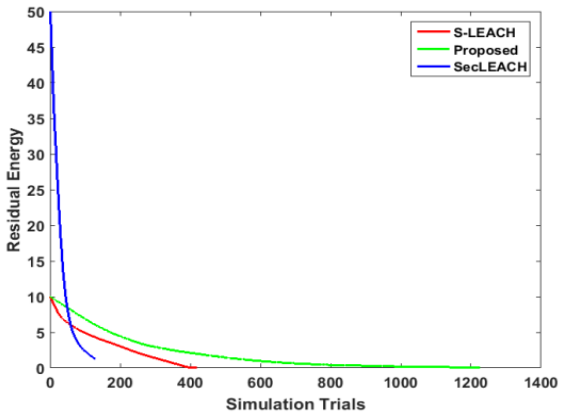

Figure 4. Comparative analysis of residual energy

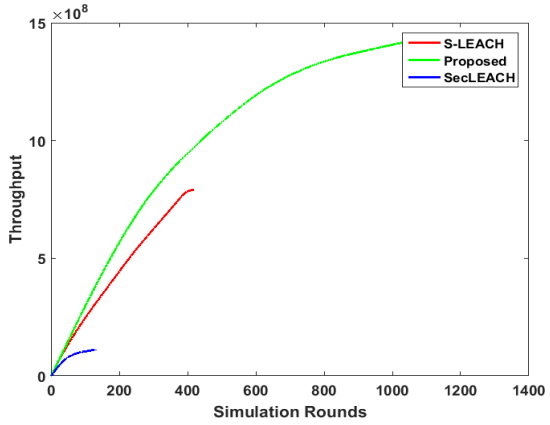

Figure 5. Comparative analysis of throughput

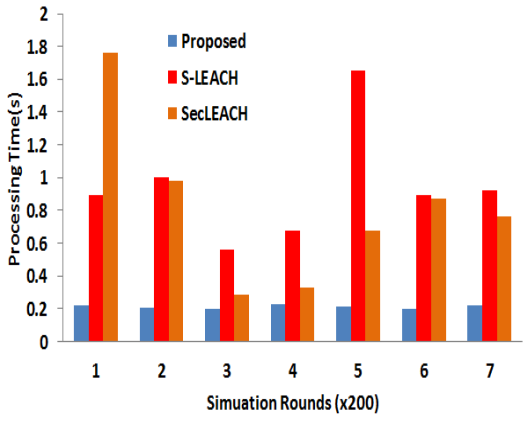

Figure 6. Comparative analysis of processing time

4. CONCLUSION

Majority of the attacks in WSN starts by compromising any of the weaker sensor nodes. Normally that starts from broadcasting the forged information within the network. The proposed system is all building a secure level of trust from the heuristics of successfully created routes and then it compares the entire incoming request for network participation. The proposed design principle after finding the presence of malicious request diverts the request using a ghost sensor. The benefit of this process is that an attacker has no other option but to rely on the forged information passed on to them by a ghost node. Hence, without using any form of encryption technique, the proposed system offers good capability to resist malicious traffic.

REFERENCES

[1] A. Sabato, C. Niezrecki and G. Fortino, "Wireless MEMS-Based Accelerometer Sensor Boards for Structural Vibration Monitoring: A Review," in *IEEE Sensors Journal*, vol. 17, no. 2, pp. 226-235, Jan. 2017.

[2] Yang K., "Wireless sensor networks: Principles, Design and Applications," Springer, 2014.

[3] Ali, Nabeel Salih, Zaid Abdi Alkareem Alyasseri, and Abdulhussein Abdulmohson, "Real-Time Heart Pulse Monitoring Technique Using Wireless Sensor Network and Mobile Application," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 8, no. 6, pp. 5118-5126, 2018.

[4] José Cecílio and Pedro Furtado, "Wireless Sensors in Heterogeneous Networked Systems: Configuration and Operation Middleware," Springer, Computers, pp. 1-143, Aug. 2014

[5] Sengar P. and Bhardwaj N., "A Survey on Security and Various Attacks in Wireless Sensor Network," *International Journal of Computer Sciences and Engineering* (IJECE), vol. 5, no. 4, pp. 78-84. 2017.

[6] Driss Benhaddou and Ala Al-Fuqaha, "Wireless Sensor and Mobile Ad-Hoc Networks: Vehicular and Space Applications," Springer- Technology & Engineering, pp. 1-248, Mar. 2015

[7] I. Butun, S. D. Morgera and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266-282, First Quarter 2014.

[8] W. Feng, Z. Yan, H. Zhang, K. Zeng, Y. Xiao and Y. T. Hou, "A Survey on Security, Privacy, and Trust in Mobile Crowdsourcing," in *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2971-2992, Aug. 2018.

[9] I. Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910-1923, Dec. 2017.

[10] A. A. Kumar S., K. Ovsthus and L. M. Kristensen., "An Industrial Perspective on Wireless Sensor Networks — A Survey of Requirements, Protocols, and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1391-1412, Third Quarter 2014.

[11] Liu, Ying, and Chunguang Li, "Secure Distributed Estimation over Wireless Sensor Networks under Attacks," *IEEE Transactions on Aerospace and Electronic Systems*, 2018.

[12] Tayebi A., Berber S., Swain A., "Security Enhancement of Fix Chaotic-DSSS in WSNs," *IEEE Communications Letters*, vol. 22, no. 4, pp. 816-819, Apr 2018.

[13] Luo M., Luo Y., Wan Y., Wang Z., "Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT," *Security and Communication Networks*, 2018.

[14] Illiano VP, Paudice A, Muñoz-González L, Lupu EC, "Determining Resilience Gains from Anomaly Detection for Event Integrity in Wireless Sensor Networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 14, no. 1, pp. 1-35, Feb. 2018.

[15] El Hajji F, Leghris C, and Douzi K, "Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks," *Journal of Communications and Information Networks*, vol. 3, no. 1, pp. 67-83, 2018.

[16] Sun Z, Xu Y, Liang G, Zhou Z., "An Intrusion Detection Model for Wireless Sensor Networks with an Improved V-Detector Algorithm," *IEEE Sensors Journal*, vol. 18, no. 5, pp. 1971-1984, Jan. 2019.

[17] Zhang K, Xu K, Wei F, "A Provably Secure Anonymous Authenticated Key Exchange Protocol Based on ECC for Wireless Sensor Networks," *Wireless Communications and Mobile Computing*, 2018.

[18] Kumar G., Rai MK, Kim HJ, Saha R., "A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks," *Mobile Information Systems,* 2017.

[19] Li J, Wang D, Wang Y., "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network," *IET Wireless Sensor Systems*, vol. 8, no. 2, pp. 68-75, Dec. 2017.

[20] Umar IA, Hanapi ZM, Sali A, Zulkarnain ZA, "Trufix: A configurable trust-based cross-layer protocol for wireless sensor networks," *IEEE Access*, vol. 5, pp. 2550-62, 2017.

[21] Guan Y. and Ge X., "Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks," *IEEE Access*, vol. 5, pp. 10858-70, 2017.

[22] Shen L, Ma J, Liu X, Wei F, and Miao M., "A secure and efficient id-based aggregate signature scheme for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 546-54, Apr. 2017.

[23] Zhang Z, Zhu H, Luo S, Xin Y, Liu X., "Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks," *IEEE Access*, vol. 5, vol. 12088-102, Jan. 2017.

[24] Ananda Kumar KS, R. Balakrishna, "Evaluation of Energy Consumption using Receiver-Centric MAC Protocol in Wireless Sensor Networks," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 8, no. 1, pp. 87-93, 2018.

[25] Nurellari E, McLernon D, Ghogho M., "A secure optimum distributed detection scheme in under-attack wireless sensor networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 2, pp. 325-37, Jun. 2018.
[26] Shafiee M, and Vakili VT., "Comparative Evaluation Approach for Spectrum Sensing in Cognitive Wireless Sensor Networks (C-WSNs)," *Canadian Journal of Electrical and Computer Engineering*, vol. 41, no. 2, pp. 77-86, 2018.
[27] Y. Liu, M. Dong, K. Ota and A. Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013-2027, Sep. 2016.
[28] Mehmood A, Khanan A, Umar MM, Abdullah S, Ariffin KA, Song H., "Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks," *IEEE Access*, vol. 6, pp. 5688-94, 2018.
[29] X. Li, J. Peng, J. Niu, F. Wu, J. Liao and K. R. Choo, "A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things," in *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606-1615, Jun. 2018.
[30] P. Gope and T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks," in *IEEE Transactions on Industrial Electronics*, vol. 63, no. 11, pp. 7124-7132, Nov. 2016.
[31] Faisal, Mohammad, Sohail Abbas, and Haseeb Ur Rahman, "Identity attack detection system for 802.11-based ad hoc networks," *EURASIP Journal on Wireless Communications and Networking,* Article no. 128 (2018), pp. 1-16, 2018.
[32] Tayebi, Arash, Stevan Berber, and Akshya Swain, "Security Enhancement of Fix Chaotic-DSSS in WSNs," *IEEE Communications Letters,* vol. 22, no. 4, pp. 816-819, 2018.
[33] Tian F, Chen X, Liu S, Yuan X, Li D, Zhang X, Yang Z., "Secrecy Rate Optimization in Wireless Multi-Hop Full Duplex Networks," *IEEE Access*, vol. 6, pp. 5695-704, 2018.
[34] El Hajji F, Leghris C, and Douzi K., "Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks," *Journal of Communications and Information Networks*, vol. 3, no. 1, pp. 67-83, Mar. 2018.
[35] Alshinina, Remah A., and Khaled M. Elleithy, "A Highly Accurate Deep Learning Based Approach for Developing Wireless Sensor Network Middleware," *IEEE Access*, 2018.
[36] Kumar, Gulshan, *et al*., "A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks," *Mobile Information Systems*, vol. 2017, 2017.
[37] Luo, M., Luo, Y., Wan, Y., & Wang, Z., "Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT," *Security and Communication Networks*, 2018.
[38] Guan, Yanpeng, and Xiaohua Ge, "Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks," *IEEE Access,* vol. 5, pp. 10858-10870, 2017.
[39] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab and A. A. F. Loureiro, "SecLEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks," *Fifth IEEE International Symposium on Network Computing and Applications (NCA'06)*, Cambridge, MA, pp. 145-154, 2006.
[40] M. El-Saadawy and E. Shaaban, "Enhancing S-LEACH security for wireless sensor networks," *2012 IEEE International Conference on Electro/Information Technology*, Indianapolis, IN, pp. 1-6, 2012.

BIOGRAPHIES OF AUTHORS

Somu Parande, completed his B.E from Karnataka University, Dharward, India and M.Tech from Mumbai University, India. He is pursuing PhD from VTU, Belagavi, Karanataka, India. His research area is Wireless Sensor Network. He has 18 years of experience in teaching.

Jayashree Mallapur, She has done B.E from Karnataka University, Dharward, India and M.Tech from Gulbarga University, India. She has completed her PhD in 2009 from VTU, Belagavi, Karanataka, India. She has 25 years of experience in teaching.