A Novel Sandboxing Framework to Identify and Resist Malicious Request using Optimization Approach in WSN

Yogeesh AC*, Shantakumar B. Patil, Premjyoti Patil***, Roopashree HR******

* Research Scholar, Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, VTU, Belagavi, Karnataka, India

**Professor, Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, VTU, Belagavi, Karnataka, India

***Professor, Department of Electronics & Communication, Nagarjuna College of Engineering and Technology, VTU, Belagavi, Karnataka, India

**** Senior Associate TRM at Publicis.Sapient at Bengaluru, Karnataka, India

Abstract— **There has been evolution of various solutions towards addressing security and energy demands of Wireless Sensor Network (WSN); however, there are less number of standard studies that has jointly addressed this problem. After reviewing existing security approaches, it was seen that there is no robust model or algorithm to identify the legitimacy of the random request of joining network in dynamic WSN applications. Hence, the proposed study introduces a simple and yet novel framework that uses a decoy sensor to resist any form of illegitimate request after they are confirmed to be malicious. The core idea is to discourage both node as well as illegal request to be joining the network. The proposed system performs routing using both single as well as multihop approach The result analysis of the study shows that proposed system offers a good balance between security demands as well as energy demands when compared with existing hierarchical secure routing approach in WSN.**

Keywords; Security, Energy, Optimization,Routin, Wireless Sensor Network.

I. INTRODUCTION

Since the past few years, wireless sensor networks (WSNs) have been widely accepted in a variety of active organizations and industrial applications due to their flexibility and low cost of service. WSN offers a wonderful and smart combination of microcontrollers, sensing device and wireless communication to serve distributed services over specific applications demand such as monitoring, tracking, etc. Thus, A WSN can formalize as a wireless network containing sink node(data center for the WSN) and clusters of miniature sensor motes equipped with fixed size battery that have a sensing ability, data processing capacity and communication among the other devices within the network through radio frequency channel [1]. Generally, the sensor motes are resource constraints(fixed limited-battery, limited storage capacity, limited sensing range and limited processing power) in nature due to their small size and low-cost factor. The objective of WSN is to monitor the environment, understand the physical world and then collect the respective information and transferred to the sink node [2]. Mostly, WSN is adopted for surveillance and security and to monitor hostile and dangerous area such as dense forest, battlefield, and where the human interaction is not possible sometimes. Moreover, nowadays WSNs are widely used in the healthcare for understanding patient behavior, battlefield, flood area to make us ready to deal the situation whenever it comes, home automation and weather forecasting [3]. Although WSN provides beneficial services with less human interaction and on other hands, it requires security consideration due to their resource constraints, and it's deployment in an unfavorable environment. The need of security mechanism becomes essential when the WSN is employed for some mission task and for a specific application that based on the real-time information. Also, due to the distributed nature of sensor nodes, the nodes cannot be considered as trustworthy, and it may compromise by an adversary with a motive to disturb the whole network operation to steal and tempering some valuable information. So, security and privacy in WSN become a primary concern to ensure the network reliability, integrity, confidentiality, authenticity and able to resist various attacks [4]. Several research works have been carried in this are that addresses the security and privacy issues in the WSN [5-7]. Providing an efficient security mechanism in resource constraints WSN is not an easy task. To tackle the security problem of resource constraints WSN, many researchers have come with some suitable security solution such as encryption, key management, secure routing protocol, etc. [8-10]. However, the privacy and security issues posed by sensor networks still represent a rich field of research problems. However, the privacy and security problems brought about by WSN are still in challenging phase and researcher's need to come with the feasible and optimized solution in order to provide a multi-objective solution. The proposed paper discusses one simple solution towards resisting threats in WSN. Section 1.1 briefs of existing security solutions, Section 1.2 briefs of research issues followed by discussion of Section 1.3 about proposed solution. Algorithm is brief in Section 2 while result is discussed in Section 3 and summary in Section 4.

II. Related Work

This section discusses the prior techniques implemented to address the problems of secure routing in the sensor network.

This section discusses the existing research works that carried in the practice of providing an effective security mechanism in WSN applications. The work carried out by the Liu et al. [11] have presented an improved distributed estimation technique based on least mean square algorithm to tackle the problem of secure estimation over WSN under the presence of attacks. Moara-nkwe et al. [12] have investigated the design and implementation problem of physical layer key generation in WSN and developed a novel secure and efficient key generation model for WSN. The results of this study show that the presented approach achieve high accuracy about 100% key agreement rate with both forward and backward security mechanism. Hasn et al. [13] have designed an optimization model for enhancing security by optimizing watchdog selection to monitor the sensor nodes in WSN. Faisal et al. [14] 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. [15] 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. [16] 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. [17] 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. [18] 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 fromWSN to end-user with utilizing optimum network resources. Kumar et al. [19] 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. [20] 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 [21] have designed Markov chain and level switching based secure model to perform a safe estimation operation under a jamming attack. Zhang et al. [22] constructed an Intrusion detection system based on self-adaptive and active trust threshold mechanism to detect malicious behavior and to control overhead problem in WSN. Nurellari et al. [23] presents, a reliable scheme for investigating the compromised nodes and to control their behaviors toward the fusion process. QIN et al. [24] introduces secure routing operations based on semiring theory to resist some common types of attacks in WSN. Li et al. [25] offers, an advanced version of the localization algorithm to overcome the problem associated with the existing Distance vector-hop algorithm under wormhole attacks. Rana [26] has presented a distributed estimation technique for controlling cyber attacks and stabilization technique for controlling packet loss in the electric vehicles. Umar et al. [27] uses a fuzzy system based secure cross-layer framework to resist some common security attacks and to provide efficient packet delivery services in the WSN. Wang et al. [28] have presented a relay and selection approach for improving security against eavesdropping attacks and also uses particle swarm optimization algorithm with simulated annealing algorithm for an appropriate node selection process. Gope et al. [29] have introduces a novel scheme to improve existing security protocols with energy efficiency and low overhead complexity for real-time WSN applications. Zhu et al. [30] have presented an overview of physical layer security in IWSNs to point out some challenges and essential requirements to improve both security and IWSN overall performance.

III. Problem Identification

The significant research problems are as follows:

- Existing techniques are found to offer more encryption-based operation that offers security but at the cost of the energy factor too among the nodes.
- Existing approaches are highly specific for specific attacks and they are not applicable of the forms of the attacks are changed.
- Authentication modeling was always carried out with respect to encryption and request matching, but legitimacy of the malicious request are yet not found to be stopped using existing technique.
- More techniques are focused on homogenous WSN and less for heterogenous WSN where the security challenges are exponentially more.

Therefore, the problem statement of the proposed study can be stated as “Developing a framework to balance security and energy demands in heterogeneous WSM is one of the most challenging optimization works”. The next section briefs of solution to address this problem.

IV. Proposed System

The prime purpose of the study is to perform optimization of the security performance of the proposed energy-efficient secure routing. The prime problem to be addressed in this phase of the work is to identify and resist the type of attack that tampers the programmes embedded in the commercial sensor application. Usually, commercial sensor applications are highly prone to various forms of unknown and anonymous service request from the adversarial node. Such adversarial nodes are quite hard to be identified and thereby it is difficult to capture / encapsulate the adversary. The complete basis of this part of the study is a new adversarial module which has the potential to access and control the programming object of the sensor node that finally leads to physical node capture. However, the scope will be only limited towards capturing programming object by the malicious node and how the proposed system resists it. The study will use similar communication model used in our prior work [31][32][33] but will introduce a novel adversarial model. The study will apply analytical modelling approach with formulation of a programming object. An authentication module will be developed which will be responsible for authenticating the challenge generated by the node. After the authentication is carried out by the node, the next step will be to apply probabilistic data structure in order to securely store the programming object of a sensor node. This phenomenon is a type of novel sandboxing mechanism that any sensor node will be using in order to secure checks the legitimacy of the incoming route request. In case of legitimate request, a secure route will be established; however, in case of illegitimate request, the sensor node is still safe as any change the programming object invokes to sandbox renders instantly the forced damage of the data structure and a new probabilistic data structure is developed.

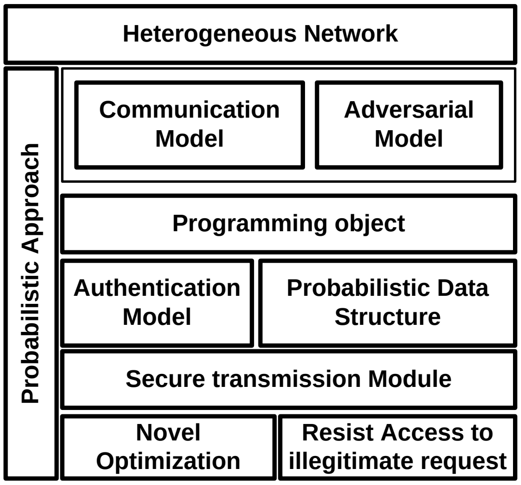

Figure 1 Indicative Scheme of Proposed System

Before, forwarding the secured routing information, the mechanism also checks for the probability of the true positive or negative in the notification generated from the sandboxing mechanism. This will be carried out in order to perform a second check on the validity of the notification about the malicious node. A novel optimization policy will be then constructed which will use an extremely lightweight cryptographic module without an extensive recursive operation in order to have better suitability with the real time sensor operation. Finally, the system will perform filtration for the legitimate and illegitimate task from the requestor node. Apart from energy and security parameters, the major aim of this part of the study will look for computational complexity of the proposed algorithm. It is expected that proposed study will maintain a better balance between energy and security incorporation.

V. ALGORITHM IMPLEMENTATION

This section discusses the implementation of the proposed algorithm that is responsible for performing a good balance between higher degree of security as well as energy efficiency using optimization approach. The core design principle of the algorithm is mainly to reduce the dependencies of using conventional encryption and offering more potential to identify the different forms of attackers. The discussion is carried out using following essentials factors of algorithm implementation:

The complete implementation is carried out over heterogeneous WSN and hence node density is considered to represent the deployed nodes. Different from any existing system, the proposed system split up the conventional 32 bit beacons into two forms of control message that bears information associated with i) message for discoving node (*msg_1*) and ii) topology related information from each adjacent nodes (*msg_2*). The first message type is used for searching node while second message type is used for controlling the topology, when demanded. The algorithm initially allows all the nodes to check the integrity of such control message that leads to selection of an auxiliary node (they are intermediate nodes used for multi-hop for forwarding messages). The novel idea of the strategy formulated is pictorially shown in Fig.2.

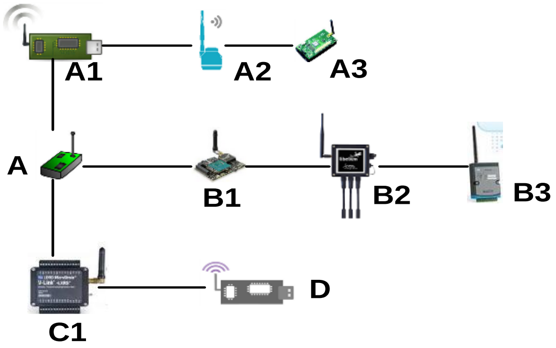

Figure 2 Scenario Considerations for Algorithm Deployment

The novelty of the proposed algorithm is that it uses a new type of a virtual node called as *decoy node* (node-D in Fig.2) that is positioned in the network in such a way that they are the highly prioritized node to be attack. According to Fig.2, the algorithm could consider following viz.i) all the sensors (A1, A2, A3, B1, B2, B3, and C) directly connected to each other, ii) node-A is considered as adversarial node that are connected with normal sensors, iii) evaluating all the neighbor sensors positioned in single hop and multiple hop of node-A, iv) the auxiliary node falls wthin single and multi-hop sensors that self declare themselves as auxiliary node. Fig.2 shows that (A1, B1, C1) are the neighboring sensors of single hop type, while (A2 and B2) are also neighboring sensors of multi-hop type. According to proposed secured routing, the node-A must choose (A1, B1) as the auxiliary sensors as it will result in protection of second hop neighboring sensors. The algorithm also consider that there is a node C1 that targets to quarantine node-A, than node-C1 must declare a msg1 as forged beacon that includes neighboring sensor list as={A, A2, B2, D}. In this case, the node-C1 will not advertise (A1, B1) because it is feasible for node-A to authenticate it by comparing msg1 of C1 with the msg1 of (A1, B1). Hence, the algorithm follows two more protocol to avoid contradiction i.e. i) *Protocol-1*: It is necessary for node-A to confirm that sensors advertised by node-C1 is not within the neighborhood list of node-A. This task takes place when node-C1 broadcast msg1 consisting of neighboring sensors of node-A. The process can be carried out by evaluating the prior *msg1* in order to check if the sensors report their source sensor as their immediate neighboring sensor. A closer look into Fig.2 will show that node-A1 and node-B1 should always retain its position as single hop neighboring nodes; therefore, node-C1 must opt auxiliary sensor that should offer accessibility to such sensor. However, in adversarial condition, there is a good possibility that node C1 may act like it want to select node A as auxiliary node itself in order to reach node A1 and node B1. In such case, node-A cannot deny the request in order to comply *non-repudiation* standards of security protocol. In this situation, the node-A cannot confirm if node C1 is actually regular or alicious node but it is possible for node-A to find out if node-C1 has already selected other auxiliary nodes in multi-hop neighboring sensors i.e. node A2 and B2. Therefore, this contradiction is solved using ii) *Protocol-2*: considering that *msg1* consist of *p*-number of sensors, than the node-A must check if there are *q*-numbers of sensors in the neighboring nodes of *p* sensors in such a way that i) there is no declaration of *msg1* of source sensor and ii) it is positions far across more number of hops from node-A. After checking this condition than it is required to be checked iii) if selected number of sensors by node-C1 are also single-hop neighboring sensors of node-C1 as well as selected as auxiliary nodes for covering *p*-sensors. Hence, the contradiction can be easily solved. The prime intention is to perform sandboxing mechanism in order to assess all the forms of request. The process of capturing the identification of an adversary (irrespective of its form) is carried out using auxiliary node itself that undertakes decision of forwarding the data as well as consider the situation under which re-transmission has to be confirmed for carryout or aborted. This process generates information that is stored in routing matrix. The algorithm assumes a presence of a unit hop between good node and decoy node. According to the scenario in Fig.2, if a node-S is attacked than any form of control message relayed by node-S will never match with the route matrix. Therefore, the decoy node does not participate in the process of communication and it is positioned to attract all the malicious traffic towards itself.

Core Algorithm Steps

The core motive of the proposed algorithm is to perform sandboxing the threats and allowing the normal communication to continue in WSN. The algorithm takes the input of A (network area), N (node density), and C_r (Communication Range) that after processing leads to generation of sec-routes (secured routes). The importants steps of the proposed algorithm are as follows:

Algorith for Sandboxing threats

Input: *A* (network area), *N* (node density), C_r (Communication Range)

Output: *sec-routes* (secured routes)

```
Start
1. init A, N, Cr
2. $R_{mat} \rightarrow f_1(p(x,y), A, N, C_r)$
3. $AN_{vec} \rightarrow f_2(N, R_{mat})$
 4. For i:1:$AN_{vec}$
5.     init $v_{node}$
6.     sec-routes$\rightarrow f_3(P(x,y), Cr, N, R_{mat}, AN_{vec})$
7. End
End
```

Following are the description of the algorithmic steps involved in proposed system:

- *Initialization*: The algorithm randomly distributes all the sensors *N* over the the area *A*. Although, all the sensors possess different networking charecteristics as well as routing properties….they are assumed to be initialized with similar value of C_r as in the later part of the simulation the sensors will start to deplete the power unevenly leading to different amount of residual energy among the sensors. It is in the initialization phase itself when the sensors are considered to be initiating the communication stage too.
- *Construction of Routing Matrix*: As discussed in prior Section 2.2, routing matrix bears all the information associated with the control messages. An explicit function $f_1(x)$ is constructed for this purpose. For all the sensors, the function obtains the positional information of sensors and computes the distance among themselves. If the distance is positive and more than zero than the function checks if the distance between two sensors are less than or equal to communication range in order to represent themselves as neighboring sensors. The function first finds all the total number of hops followed by segregatting the single hop to double hop. All the respective information of the hops is then strored in a variable called as route matrix R_{mat} (Line-2). The significance of R_{mat} table is that it retains all forms of hop-based information that will be required in the next stage of evaluation where the target node will check the authenticity of a sensor on the basis of the presence of hop information within route matrix table i.e. R_{mat}.
- *Identification of Auxilliary Sensor*: The significance of auxiliary sensor is that it constructs a decision of packet forwarding as well as retransmission. Basically, it is a special operation given to a sensor by accessing route matrix and that leads to decision making. However, if a compromised node is selected as an auxiliary node than chances of getting the complete network compromised is very high. An explicit function $f_2(x)$ is constructed (Line-3) that takes the input of number of sensor *N* and route matrix R_{mat} in order to generate a communication vector for auxiliary node. The operation of the function is as follows: For the entire sensor *N*, the function $f_2(x)$ obtains the information of all the sensors retained within the route matrix R_{mat} and the obtained information. The next phase

of the study is to identify the neighboring nodes of multihop type as well as single hop type. This operation is followed by remodeling the routing matrix R_{mat} in such a way that only the adjacent nodes lying witin second hop is considered and then single hop is extracted from them. The advantage of this process is that it offers comprehensive information of a link leading from the target node with presence of both single and double hops. Only the unique links are stored back in the routing matrix now. The common elements of the both unique single hop and double hop links are explored and communication vector is obtained. The next part of the processing attempts to find the coverage of such sensors where a sensor with single hop is extracted followed by exploring the common values between the single and double hop neighboring nodes. All the coverage vectors are then sorted that finally offers multiple way of representing that the selected node can be now chosen as an auxiliary node and they are also compliant of both the protocols mentioned in prior sub section of 2.1. *Constructing a Secured Route*: The complete implementation of this algorithm starts when the decoy node D becomes functional. The proposed study implements a unique adversarial model where it is assumed that they are highly potential of invoking physical attacks over the nodes. It is also considered that the adversary will increase its gain by trying to compromise a sensor with higher number of associated links (i.e.multihops). So, for this purpose, an explicit function $f_3(x)$ is designed that takes the input of position of sensors, communication range, sensors, routing matrix, and coverage vector of auxiliary node (Line-6) in order to formulate secured routes. It does so by allowed the framework to initialize the number of victim nodes v_{nodes} (Line-5). Following are the operations performed by the function $f_3(x)$: For all the number of sensors *N*, the address of the local routes are saved in routing matrix and it assesses if address of the local node is equivalent to the destination sensor. In case of positive match, the consecutive address of the hop is saved along with periodic updating in routing matrix as well as address of local sensor. It is then followed by saving the number of hops over the routing matrix. However, if the match between address of local sensor and destination node than *msg1* is first extracted from the address of the local sensor followed by exploring all the single hop neighboring sensors of the local network. It is found from its *msg1* itself. The next step is to look for presence of single hop for similar way followed by identification of the nearest auxiliary node. The algorithm has focused on using *msg1* itself till this step, but now, it will use *msg2* in order to ensure security factor associated with controlling topology. The control message *msg2* is obtained from single hop neighboring sensors followed by identification of addresses of local sensor as the auxiliary node from the single hop nodes. From this, the presence of *msg2* is checked by evaluating the presence of set of selected auxiliary node for a sensor. In case the auxiliary nodes are present than the spatial distance between the corresponding auxiliary nodes as well as destination nodes are computed. Finally, the nodes with minimal distance are shortlisted for formulate secured routes at the end.

A closer look into the implementation strategy of proposed system will thereby show that usage of decoy node can be used for resisting the attacks as decoy node after identifying the form of request broadcast all the fake routes that never exists. The information offered by decoy nodes visibly looks so confusive that any adversary will add forged information of multihop routes that literally doesn’t exist. This operation results in allocation of network and computational resources of attackers towards attacking the node that doesn’t exists and set for travelling a path that doesn’t exist. This operation will result in even a packet drop as well as faster resource consumption for the attacker node itself. Another interesting part to be seen here is that although the role of auxiliary node is very important but it shouldn’t be used in more numbers as it may over overheads. This problem is restricted by invoking a threshold that limits the need of auxiliary node. Another observation of proposed algorithm is that it offers significant level of security without using encryption as well as without using any logic that has external resource or entity dependencies. Hence, the proposed system truelly offers a robust optimization-based logic in its algorithm where without increasing any dependencies as well as any prior definition of attacks, the proposed system offers capability to identify and stop all forms of malicious communication along with deviating them. The next section outlines the results accomplished.

VI. RESULT ANALYSIS

This section discusses about the results obtained after implementing the proposed algorithm. The assessment of this algorithm is carried out considering 100 sensor nodes considering variable communication range of 10-40m. The scripting of the proposed logic was carried out in MATLAB. As the proposed scheme is mainly concern about security and energy efficiency via the optimization principle; therefore, the outcome of the proposed system was compared with the existing secured Leach [34] protocol as a standard benchmarking.

.

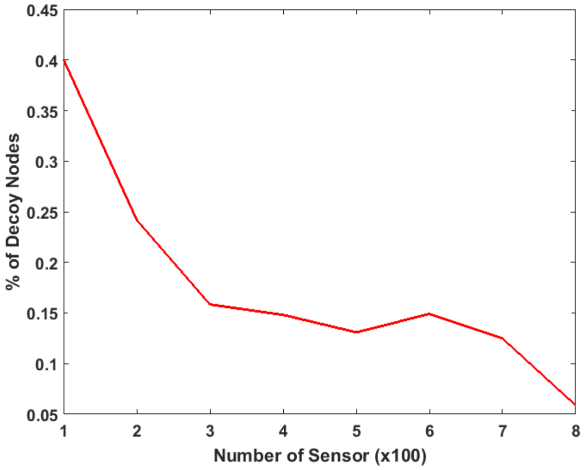

Figure 3 Analyses of Decoy Node Dependencies

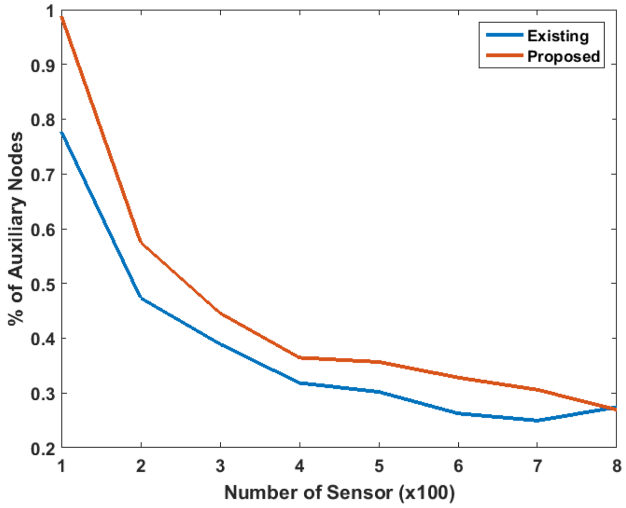

Figure 4 Comparative Analyses of Auxiliary Nodes

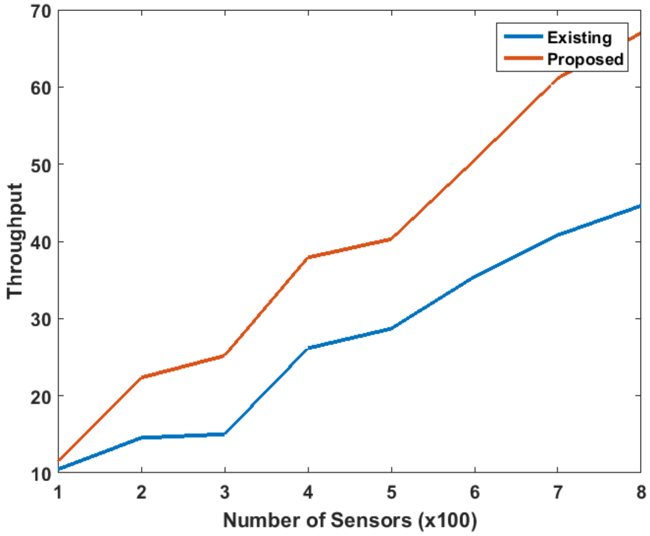

Figure 5 Comparative Analysis of Throughput

The interpretation of the outcomes obtained from the result analysis is as follows:

- Analysis of Decoy Nodes: A true meaning of optimization wil highlight about obtaining the best result without using any external resource or entities. Basically, a decoy node is one of the node out of all the sensor nodes deployed and is considered to be acting as ghost node when it is demands. By ghost node, it will mean that it should possess a capability to mask its local address and further initiate broadcasting forged information to show that it is the only node that knows the information about the multihop connection. Moreover, the broadcast of its neighborhood are too forged and it never is meant to be broadcasted for original neighbor nodes. Hence, there is zero overhead because of broadcasting operation of decoy nodes. Fig.3 shows that with increase of sensor density, such dependencies decreases for proposed system, which truly mean successful optimization.
- Analysis of Auxiliary nodes: It should be known that decoy node is meant for resisting the entry of malicious request while auxiliary node is to ensure that a requestor node always obtain good content of information about the better route possibilities. However, auxiliary node is the only node that is demanded when a decision of routing or retransmission has to take place. Hence, it is evident that they will consume more amounts of energy and other resources too. The outcome shown in Fig.4 highlights that dependency of auxiliary node reduces down with increase of sensor population. It should be known that such dependencies of auxiliary node is only required when a clusterhead is required to find a way to reach the next clusterhead in case of abnormal traffic. After analysis, it shows that proposed system offers better routing performance and doesn't require too many dependencies on auxiliary nodes, although initially it has some dependencies. The performance of SecLEACH as well as proposed system is nearly same; however, proposed system shows slightly higher dependencies of auxiliary nodes, which are in tolerable limits and is capable of offering better optimization performance owing to zero encryption approach.
- *Analysis of Throughput*: One of the best part of the proposed system is its capability to forward the packet. The analysis in Fig.5 shows that throughput performance of proposed system is much better as compared to existing SecLEACH algorithm. The main reason behind this is proposed system doesn't use any form of iterative function like that used in SecLEACH algorithm and moreover with the existence of routing matrix, the decision taken by all the nodes as well as auxiliary nodes offers a comprehensive routing plan that leads the network to process the data packer faster in highly secured manner without using conventional encryption-based approach.

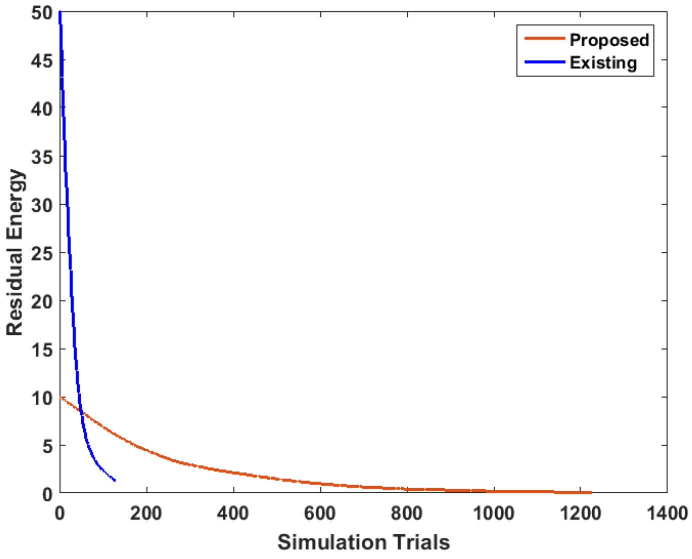

Figure 6 Comparative Analysis of Energy Depletion

- *Analysis of Energy Depletion*: All the activity carried out by proposed system is mainly related to checking the control messages *msg1* and *msg2*. Based on this, every routing and accessibility decision are undertaken by the sensors. With increasing simulation, the network gain more information owing to presence of auxiliary nodes which is responsible for lowering the network overhead. Moreover usage of probability parameter further assists in faster computation and lower iterative operation that results in very slower pace of energy consumption for proposed system. However, SecLeach is not found to offer much resistivity against energy drainage and hence it shows faster degradation of energy thereby reducing the network lifetime in WSN. Hence, proposed system offers better energy efficiency over increased period of time.

VII. CONCLUSION

The proposed system offers a novel sandboxing mechanism that uses a decoy node as an essential sandboxing element. Upon identification of the malicious request, the proposed system uses the decoy node to broadcast all the forged routes as well as nodes that don’t exist at all. This oeration not only identifies the malicious nodes but also diverts such traffic thereby protecting the core networks. The contribution of the proposed system are: i) it offers a simple and yet robust optimization towards both security as well as energy, ii) it offers resistance using both single and multiple hops showing supportabiity of different routing scheme, iii) it offers very less energy consumption compared to standard secure and energy efficient algorithm.

REFERENCES

[1]. Yang, Kun. "Wireless sensor networks." Principles, Design and Applications (2014).

[2]. L. Song and D. Hatzinakos, "Architecture of Wireless Sensor Networks With Mobile Sinks: Sparsely Deployed Sensors," in IEEE Transactions on Vehicular Technology, vol. 56, no. 4, pp. 1826-1836, July 2007.

[3]. Stankovic, John A., Anthony D. Wood, and Tian He. "Realistic applications for wireless sensor networks." Theoretical aspects of distributed computing in sensor networks. Springer, Berlin, Heidelberg, 2011. 835-863.

[4] Roopashree H.R. and A. Kanavalli, "STREE: A Secured Tree based Routing with Energy Efficiency in Wireless Sensor Network," 2015 International Conference on Computing and Communications Technologies (ICCCT), Chennai, 2015, pp. 25-30.

[5].Azzabi, Tarek, Hassene Farhat, and Nabil Sahli. "A survey on wireless sensor networks security issues and military specificities." Advanced Systems and Electric Technologies (IC_ASET), 2017 International Conference on. IEEE, 2017.

[6].Almomani, Iman, and Mamdouh Alenezi. "Efficient Denial of Service Attacks Detection in Wireless Sensor Networks." J. Inf. Sci. Eng. 34.4 (2018): 977-1000.

[7]. Al-Janabi, Samaher, et al. "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications." Egyptian Informatics Journal 18.2 (2017): 113-122.

[8]Yu, Fei, et al. "Recent Advances in Security and Privacy for Wireless Sensor Networks 2016." Journal of Sensors 2017 (2017).

[9].Ishmanov, Farruh, and Yousaf Bin Zikria. "Trust mechanisms to secure routing in wireless sensor networks: current state of the research and open research issues." Journal of Sensors 2017 (2017).

[10]Poriye, Monika, and Shuchita Upadhyaya. "DNA-Based Cryptography for Security in Wireless Sensor Networks." Cyber Security: Proceedings of CSI 2015. Springer Singapore, 2018.

[11]. Y. Liu and C. Li, "Secure Distributed Estimation Over Wireless Sensor Networks Under Attacks," in IEEE Transactions on Aerospace and Electronic Systems, vol. 54, no. 4, pp. 1815-1831, Aug. 2018.

[12] K. Moara-Nkwe, Q. Shi, G. M. Lee and M. H. Eiza, "A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks," in IEEE Access, vol. 6, pp. 11374-11387, 2018.

[13].M. M. Hasan and H. T. Mouftah, "Optimization of Watchdog Selection in Wireless Sensor Networks," in IEEE Wireless Communications Letters, vol. 6, no. 1, pp. 94-97, Feb. 2017.

[14].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 2018.1 (2018): 128.

[15]Tayebi, Arash, Stevan Berber, and Akshya Swain. "Security Enhancement of Fix Chaotic-DSSS in WSNs." IEEE Communications Letters 22.4 (2018): 816-819.

[16]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. 2018;6:5695-704.

[17]El Hajji F, Leghris C, Douzi K. Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks. Journal of Communications and Information Networks. 2018 Mar 1;3(1):67-83.

[18].Alshinina, Remah A., and Khaled M. Elleithy. "A Highly Accurate Deep Learning Based Approach for Developing Wireless Sensor Network Middleware." IEEE Access (2018).

[19].Kumar, Gulshan, et al. "A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks." Mobile Information Systems 2017 (2017).

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

[21].Guan, Yanpeng, and Xiaohua Ge. "Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks." IEEE Access 5 (2017): 10858-10870.

[22].Z. Zhang, H. Zhu, S. Luo, Y. Xin and X. Liu, "Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks," in IEEE Access, vol. 5, pp. 12088-12102, 2017.

[23]. Nurellari, Edmond, Des McLernon, and Mounir Ghogho. "A secure optimum distributed detection scheme in under-attack wireless sensor networks." IEEE Transactions on Signal and Information Processing over Networks 4.2 (2018): 325-337.

[24].Qin D, Yang S, Jia S, Zhang Y, Ma J, Ding Q. Research on trust sensing based secure routing mechanism for wireless sensor network. IEEE Access. 2017;5:9599-609.

[25].Li, Jianpo, Dong Wang, and Yanjiao Wang. "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network." IET Wireless Sensor Systems 8.2 (2017): 68-75.

[26] M. M. Rana, "Attack Resilient Wireless Sensor Networks for Smart Electric Vehicles," in IEEE Sensors Letters, vol. 1, no. 2, pp. 1-4, April 2017, Art no. 5500204.

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

[28].K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo and Y. Sun, "Strategic Antieavesdropping Game for Physical Layer Security in Wireless Cooperative Networks," in IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9448-9457, Oct. 2017.

[29]. Gope, Prosanta, Jemin Lee, and Tony QS Quek. "Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks." IEEE Sensors J. 17.2 (2017): 498-503.

[30]. J. Zhu, Y. Zou and B. Zheng, "Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks," in IEEE Access, vol. 5, pp. 5313-5320, 2017.

[31] A. C. Yogeesh, S. B. Patil and P. Patil, "A Survey on Energy Efficient, Secure Routing Protocols for Wireless Sensor Networks", International Journal of Engineering and COmputer Science, Vol.5, No.8,2016

[32] A. C. Yogeesh, S. B. Patil and P. Patil, "FEESR: Framework for energy efficient secured routing in heterogeneous sensor network," 2016 International Conference on Circuits, Controls, Communications and Computing (I4C), Bangalore, 2016, pp. 1-7.

[33] Yogeesh A.C., Patil S.B., Patil P., Roopashree H.R. (2019) DSP-IR: Delay Sensitive Protocol for Intelligent Routing with Medium Access Control. In: Silhavy R. (eds) Cybernetics and Algorithms in Intelligent Systems. CSOC2018 2018. Advances in Intelligent Systems and Computing, vol 765. Springer, Cham.

[34] 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, 2006, pp. 145-154.