iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39234

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

Performance Analysis of Wireless Sensor Networks Based on Trust Mechanism

Subiksha.V[1], Dr. S. Karthikeyan[2]
[1] *PG Student,* [2]*Professor, Department of Electronics and communication Engineering, KSR College of Engineering, Tamil Nadu, India*

Abstract: ***Due to the characteristics like limited resources and dynamic topology, wireless sensor networks (WSNs) are facing two major problems such as security and energy consumption. To deal with various improper behaviors of nodes the trust-based solutions are possible but still exist a variety of attacks, high energy consumption, and communication congestion between nodes. Therefore, this paper proposes an advanced and efficient trust-based secure and energy-efficient routing protocol (TBSEER) to solve these network problems and to avoid malicious nodes. Efficient Adaptable Ant Colony Optimization Algorithm (EAACO) calculates the comprehensive trust value through adaptive direct trust value, indirect trust value, and energy trust value, which can be resistant to internal network attacks such as sinkhole, black hole, selective forwarding, and hello flood attacks. In addition, to fast identify the malicious nodes in the WSN, the adaptive penalty mechanism and volatilization factor are used. Moreover, the nodes only need to calculate the direct trust value, and the indirect trust value is obtained by the sink, so as to further reduce the energy consumption caused by iterative calculations. To actively avoid network attacks, the cluster heads find the safest multi-hop routes based on the comprehensive trust value. The simulation results show that the proposed EAACO reduces network energy consumption, speeds up the identification of malicious nodes, as well as resists all common attacks.***
Keywords: Comprehensive trust value, direct trust value, indirect value, EAACO, network attacks, wireless sensor networks

I. INTRODUCTION

In the recent years, with the rapid development of Internet of Things (IoT), WSN has been more and more widely used in military, environmental monitoring, medical and industrial production, traffic control and other fields. WSNs are composed of numerous sensor nodes, which can collect data from the environment and sends the collected data to the Sink hop by hop. The main aspects to be considered in the research and application due to the characteristics of nodes, such as small size, limited memory, computing power and energy, the low energy consumption and low cost of nodes. In addition to that, WSNs are also deployed in the unattended and unfriendly environment, which makes them unsafe to a variety of network attacks. Especially, there is no fixed topology [9] in WSNs, and each node needs to have the function of routing to forward data. Therefore, the nodes are at risk to various network routing attacks. To defend against network routing attacks from malicious nodes has become a trending topic in WSNs.

So, in order to guarantee the routing security of wireless sensor networks, many researchers have proposed kinds of secure routing protocols based on cryptography and authentication. Based on cryptography and identity verification security mechanism is not appropriate to deal with bad behavioral attacks of malicious nodes. Because implementing these security mechanisms is that all nodes are cooperative and trustworthy, which is unrealistic for internal attacks on the network and these mechanisms will also require complex calculations and high memory capacity, which additionally leads to high energy consumption. Therefore, this paper proposed trust perception-based security mechanisms to solve the problems in the security mechanisms based on encryption and identity verification.

II. EXISTING SYSTEM

To defend against routing attacks in WSNs, especially internal attacks, the security mechanisms based on trust awareness have been verified to be effective. But the traditional trust management system also has various problems. For example, when calculating the trust value for neighbor nodes like in references [1], nodes have frequent communication with neighbor nodes, resulting in information congestion, high energy consumption and long end-to-end delay [7]. At the same time, the traditional trust management system like in references [5,6,8] only considers a single type of defense attacks and cannot quickly detect malicious nodes.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

III. PROPOSED SYSTEM

Efficient Adaptable Ant Colony Optimization Algorithm (EAACO) is proposed to solve the above-mentioned internal network problems. An efficient evaluation of trust perception model is proposed in this paper, which can estimate the node's trust value derived from its behaviour to identify or isolate the malicious nodes effectively. The trust mechanism model is introduced into the efficient and optimizing ant colony routing algorithm to improve the security for data forwarding.

1) To improve the accuracy of trust evaluation and the speed of identifying malicious nodes, nodes use adaptive penalty coefficient and volatility factor with space and time constraints to calculate the direct trust value.
2) To reduce the information congestion and energy consumption with many neighbor nodes, the sink calculates the comprehensive trust value of the trusted neighbor nodes based on the direct trust value sent by the nodes, while the indirect trust value calculation is done by frequent communication.
3) By establishing inspector nodes, the behaviors of member nodes and cluster heads in the clusters are monitored. A safe route can be selected from the multiple paths which can actively avoid wormhole attacks from malicious nodes in the network.
4) To improve the security of the network and enhance the ability to resist a variety of common attacks, a new trust model and secure routing have been constructed.

IV. MODULE DESCRIPTION

A. Decryption of Intermediate

In reference [2], a secure end-to-end routing protocol is proposed, which has a special group key pre-distribution scheme. To remove the encryption and decryption of intermediate sensors, the proposed protocol uses path keys thereby protecting routing data and reducing the time required for intermediate sensors to process data. Specifically, reference [1] does not use multiple pairs of shared keys to repeatedly perform encryption and decryption on each link, but uses a unique end-to-end path key. In addition, the proposed trust mechanism protocol has good performance in correctness, freshness of authentication response, freshness of communication key.

B. Trust Management Scheme

The internal attacks have not been considered in these methods mentioned above. Therefore, trust-based security mechanism is proposed to deal with different internal attacks. In reference [3] a lightweight trust management scheme (LTMS) based on binomial distribution is proposed, which focuses on the design of trust model and the selection of cluster heads. The proposed trust model is composed of direct and indirect trust value, which is used to select and update the cluster heads. In reference [18], a trust-based fuzzy implicit cross-layer protocol (TrufiX) is proposed. TrufiX uses multiple parameters extracted through information exchange between layers to mitigate the impact of network security threats. The proposed protocol consists of two fuzzy logic systems (FLS) in series. The first FLS considers distance, trust and response time to determine the appropriateness of nodes.

C. Malicious Behavior

In order to save energy and improve security, this paper proposes EAACO whose historical trust value is volatilized under the volatilization factor and malicious behavior is punished under adaptive penalty coefficient, so as to improve the accuracy of the trust model. The direct trust value, indirect trust value and energy trust value are used to evaluate the comprehensive trust value, then the node's security is evaluated. Therefore, it can resist various attacks such as black hole, selective forwarding, sinkhole and hello flood attacks of malicious nodes. Consequently, the nodes with high security in the network and high residual energy are selected as cluster heads (CHs) according to the comprehensive trust value. Finally, according to the comprehensive trust value and transmission distance, the security of the routing paths is evaluated to find the best one that can actively defend against wormhole attack.

D. Trust Model

As in references [3],[4], nodes identify malicious nodes by calculating trust values. The key to protecting routing is to improve the trust value of normal nodes and quickly reduce the trust value of malicious nodes. Therefore, this paper uses the adaptive penalty coefficient to quickly reduce the trust value of malicious nodes, so as to achieve the purpose of quickly identifying malicious nodes and fast eliminating malicious nodes. Therefore, in order to avoid the transmission of a large amount of query information between nodes, this paper adopts a centralized computing mode to reduce the burden on nodes. The indirect trust value of all nodes is calculated by the Sink, and each node only needs to attach the direct trust value to the neighbor node in the data packet, and then send it to the Sink, so there will be no extra energy consumption.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

E. Network Model

Before elaborating the design of secure routing, certain assumptions about the basic model of the network, was made that includes: (i) Sensor nodes are randomly deployed in the network to detect the surrounding environment. (ii)Each sensor node has the same initial energy, computing power and storage capacity, and is static. (iii)The Sink is static and has unlimited resources. (iv)After node deployment, the Sink knows the unique identifier (ID) and location information of each node. The network is composed of different sized clusters and each cluster is composed of three types of nodes: member nodes (MNs), cluster heads (CHs) and inspector nodes (INs).

F. Ant colony optimization algorithm

The ant colony optimization algorithm is an algorithm for finding optimal paths that is based on the behavior of ants searching for food. At first, the ants wander randomly. When an ant finds a source of food, it walks back to the colony leaving "markers" (pheromones) that show the path has food.

In the first step of solving a problem, each ant generates a solution. In the second step, paths found by different ants are compared and in the third step, paths value or pheromone is updated. There are many optimization problems where Ant Colony Optimization (ACO) is used for finding the optimal solution.

An ant will move from node i to node j with probability,

$$pi,j = (\tau_{i,j}{}^{\alpha})(\eta_{i,j}{}^{\beta}) / \sum (\tau_{i,j}{}^{\alpha})(\eta_{i,j}{}^{\beta})$$

where,

$\tau_{i,j}$ is the amount of pheromone on edge i, j

α is a parameter to control the influence of $\tau_{i,j}$

$\eta_{i,j}$ is the desirability of edge i, j (typically 1/di,j)

β is a parameter to control the influence of $\eta_{i,j}$

Amount of pheromone is updated according to the equation,

$$\tau_{i,j} = (1 - \rho)\, \tau_{i,j} + \Delta\, \tau_{i,j}$$

where,

$\tau_{i,j}$ is the amount of pheromone on a given edge i, j

ρ is the rate of pheromone evaporation

$\Delta\, \tau_{i,j}$ is the amount of pheromone deposited, typically given by

$$\Delta\tau\, k_{i,j} = (\, 1/L_k \text{ if ant k travels on edge i, j}$$

0 otherwise)

where, L_k is the cost of the k_{th} ant's tour (typically length).

Pheromone values are updated by all the ants that have completed the tour.

$$\tau_{i,j} \leftarrow (1 - \rho) \cdot \tau_{i,j} + \sum^{m}{}_{k=1}\, \Delta\tau^{k}_{ij}\,,$$

where,

ρ is the evaporation rate

m is the number of ants

$\Delta\tau^{k}_{ij}$ is pheromone quantity laid on edge (i, j) by the k_{th} ant

$$\Delta\tau\, k_{i,j} = (\, 1/L_k \text{ if ant k travels on edge i, j}$$

0 otherwise)

where, L_k is the tour length of the k_{th} ant.

V. SIMULATION RESULTS

In this section, the performance analysis of TBSEER is compared with TSSRM and TESRP, the existing protocol models in VMware workstation with front end of ns2 script. The simulation time is based on round, and the malicious nodes can attack the network by the networks like black hole, selective forwarding, sinkhole, hello flood and wormhole attacks in the simulations. When the network runs to the 100th round, the malicious nodes invade the network and launch attacks successfully. Fig.1. Shows the design of the simulation network in VMware workstation.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

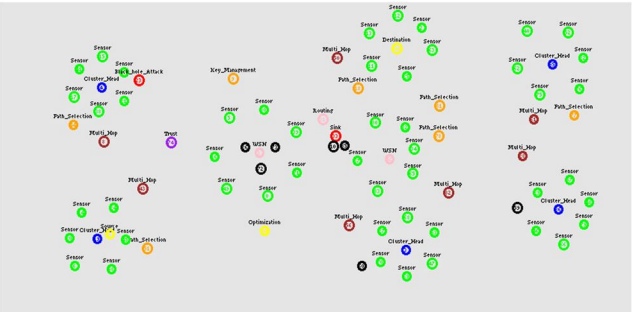


Fig. 1. Design of the simulation network

A. Comprehensive Trust Value of Malicious Nodes Under Attack

The comprehensive trust value represents the security of nodes. As long as the comprehensive trust value is lower than the threshold, the nodes are malicious. Fig.1. shows the change of comprehensive trust value of malicious nodes under different malicious attacks.

1) Black hole attacks
2) Selective forwarding attacks
3) Sinkhole attacks
4) Hello flood attacks
5) Wormhole attacks

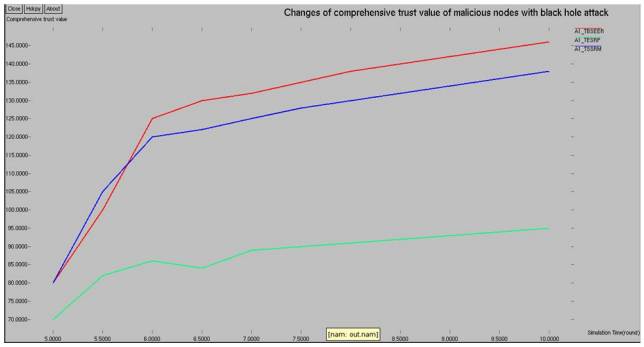


Fig.2. (a) changes of comprehensive trust value of malicious nodes with black hole attack

Black hole attack occurs, when an intermediary captures and re-programs a set of nodes in the network to block/drop the packets and generates false messages instead of forwarding correct information towards the base station in wireless sensor network.

When the network runs, malicious nodes launch black hole attacks and the comprehensive trust value decreases as the network runs. Fig. 2(a) shows the ability that three security mechanisms resist malicious nodes when they launch black hole attacks. It can be seen from Fig. 2(a) that the security mechanism in TBSEER is the optimal. Compared with TESRP and TSSRM, the performance of TBSEER against black hole attack is increased by 74% and 61.1%, respectively.

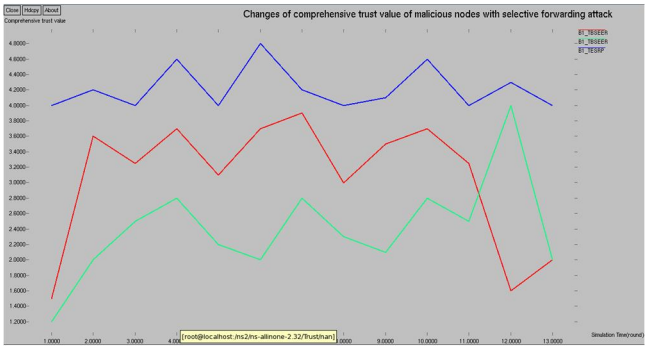


Fig. 2. (b) Changes of comprehensive trust value of malicious nodes with selective forwarding attack

In a selective forwarding attack, the malicious node which participates in the routing as normal node, selectively discards packets from neighboring nodes. These malicious nodes may forward non-critical data normally, but drop the important data. Compared with black hole attack, selective forwarding attack is more difficult to identify in the network.

Fig.2 (b) shows the ability that three security mechanisms resist malicious nodes when they launch selective forwarding attacks. It can be seen from Fig. 2(b) that TBSEER to counter the selective forwarding attacks before it can be excluded from the network. Compared with TESRP and TSSRM, the performance of TBSEER against selective forwarding attacks increased by 40.8% and 25%, respectively.

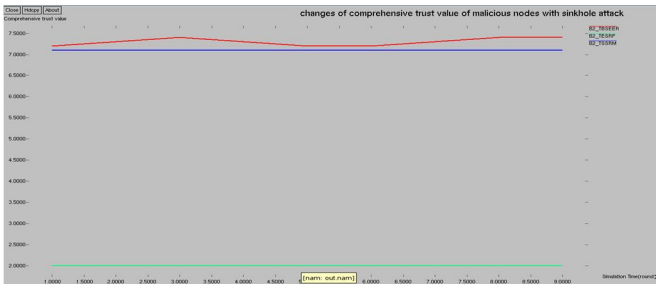


Fig. 2 (c) changes of comprehensive trust value of malicious nodes with sinkhole attack

One of the impacts of sinkhole attack is that, it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack and drops or altered routing information. In order to reduce the damage of this attack from the network and speed up the malicious nodes to be recognized TBSEER introduces an adaptive penalty coefficient, which makes the more times of malicious behavior, the stronger the penalty effect, and quickly reduces the trust value of malicious nodes. It can be seen from Fig. 2(c) that TESRP and TSSRM cannot detect the counter of the sinkhole attacks in the network. Compared with TESRP and TSSRM, the performance of TBSEER against selective forwarding attack increases by 7.5% before it can be excluded from the network.

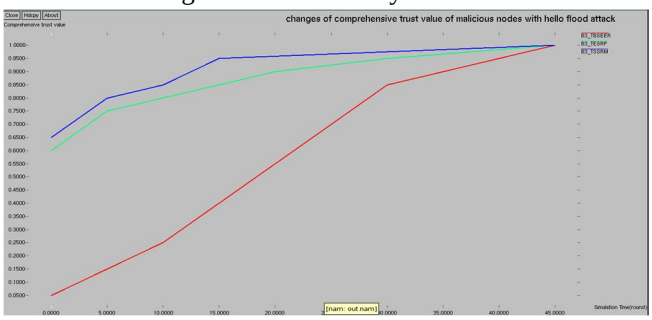


Fig.2.(d) changes of comprehensive trust value of malicious nodes with hello flood attack

Next is the verification of the performance of three trust-based security schemes under the hello flood attack. As shown in Fig.2.(d), under the resistance of TBSEER, the comprehensive trust value of malicious nodes drops below the threshold the fastest, so the security of TBSEER is most effective. Compared with TSSRM and TESRP, the performance that TBSEER against hello flood attacks has increased by 20% and 60%, respectively.

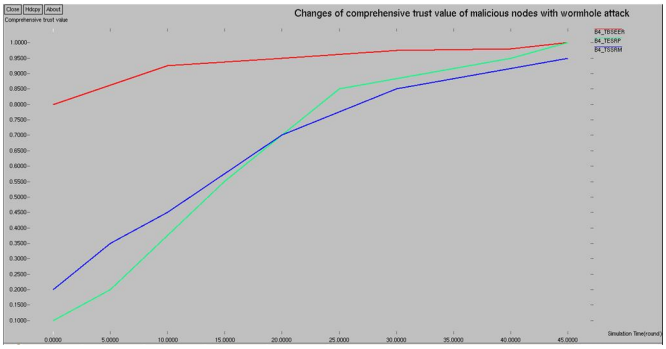


Fig.2. (e) changes of comprehensive trust value of malicious nodes with wormhole attack

Finally, the verification ability of TBSEER, TSSRM and TESRP to resist wormhole attack can be seen from Fig. 2(e). The comprehensive trust values of malicious nodes for TSSRM and TESRP are not reduced. It shows that under the protection mechanism of TSSRM and TESRP, the trust that the result of malicious nodes being evaluated by the network is still very high, and the wormhole attack initiated by malicious nodes cannot be detected. However, when 2% of malicious nodes launch wormhole attacks, TBSEER only needs 8 rounds to exclude them from the network.

B. Energy Consumption on Calculating Indirect Trust Value

In the proposed trust model, the direct trust value provided by the third-party nodes participates in node updating and calculating the indirect trust value of neighbors. Therefore, the trust model has produced a certain communication cost.

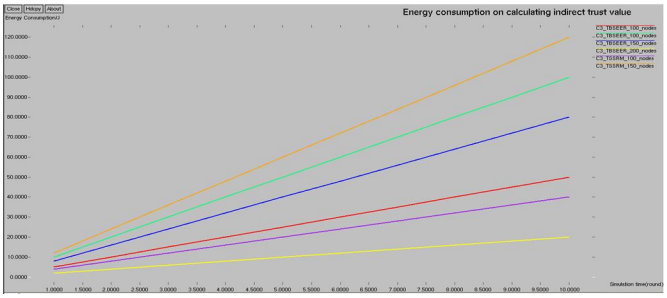


Fig.3.Energy consumption on calculating indirect trust value

Fig.3. shows the energy consumption on calculating the indirect trust value in different environments. TBSEER uses the sink with unlimited energy and powerful functions to update and calculate the indirect trust value. The Sink shares the load of the nodes and saves the energy of the nodes in the wireless sensor network. In addition, the energy consumption of nodes increases with the number of nodes in the network. However, the performance of TBSEER is still better than TSSRM and TESRP by 60%.

VI. CONCLUSION

This paper proposes a new trust based secure and energy efficient routing protocol in Efficient Adaptable Ant Colony Optimization Algorithm (EAACO) to deal with various common network attacks. It is of great significance to provide security and energy saving routing paths in resource-constrained wireless sensor networks. The target of EAACO is to improve the security of the network as much as possible while saving the network energy consumption. EAACO presents a new trust model, which considers the influence of the volatilization factor and adaptive penalty coefficient. It can accelerate the identification speed of malicious nodes and effectively identify black hole, selective forwarding, sinkhole and hello flood attacks. In addition, the nodes find a safe and energy-saving route based on the trust model in a multi-path search method, which actively avoids wormhole attack. The simulation results in VMware workstation show that compared with the traditional trust-based mechanisms, EAACO can reduce routing overhead and improve data transmission reliability.

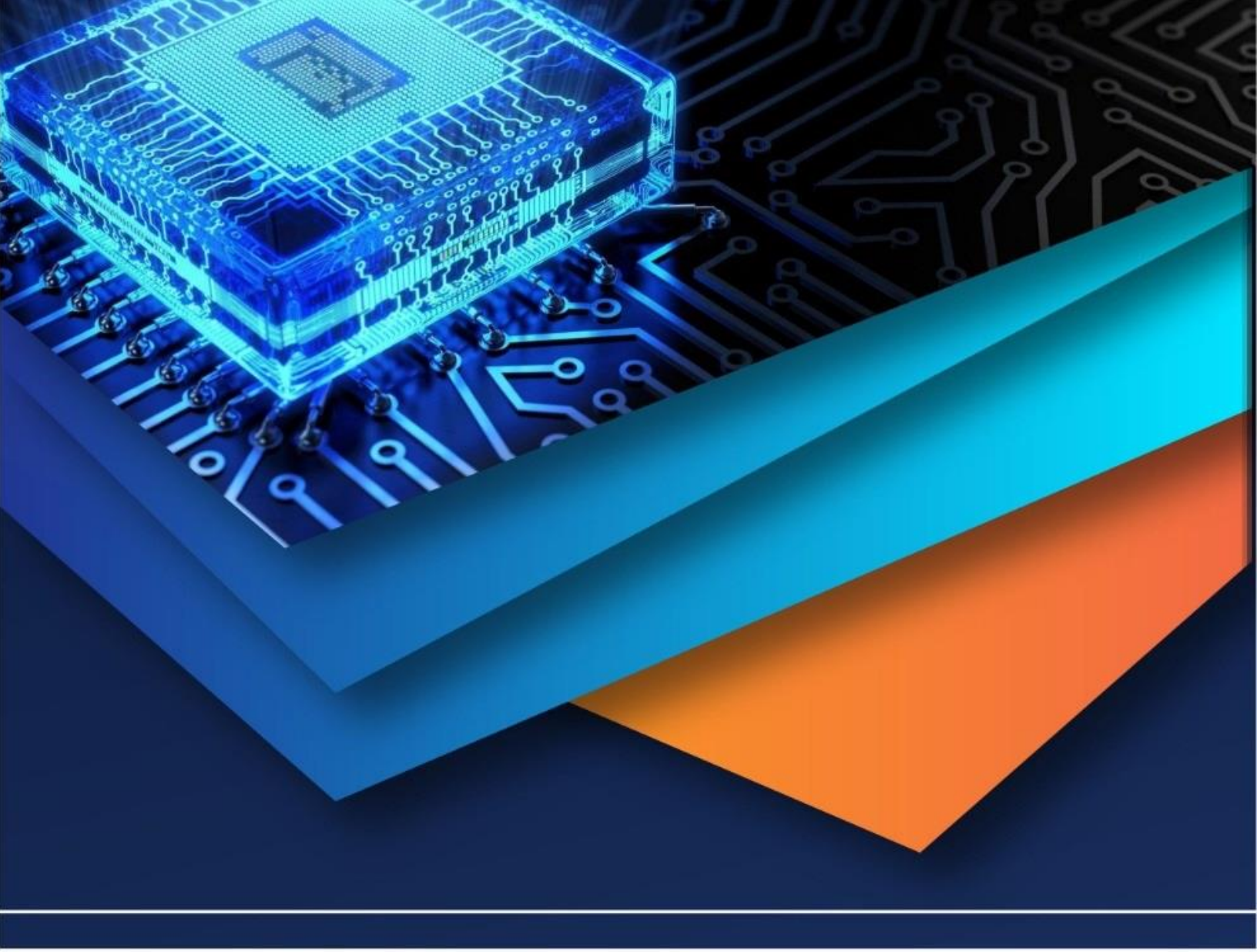
All the acronyms mentioned in this paper are listed in below Table I.

TABLE I
DEFINITION OF ACRONYMS

WSNs	Wireless Sensor Networks
TBSEER	Trust Based Secure Energy Efficient Routing
EAACO	Efficient Adaptable Ant Colony Optimization
ACO	Ant Colony Optimization
TSSRM	Trust Sensing based Secure Routing Mechanism
TESRP	Trust and Energy Aware Security Routing Protocol
FLS	Fuzzy Logic Systems
LTMS	Lightweight Trust Management Scheme
ID	Identifier
MN	Member Node
CH	Cluster Head
IN	Inspector Node

REFERENCES

[1] Huangshui Hu, Youjia Han, Meiqin Yao and Song Xue, "Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks", Institute of Electrical and Electronics Engineers Access, 2019.
[2] Muthu Senthil B, Kim H. "SHRP-Secure Hybrid Routing Protocol over Hierarchical Wireless Sensor Networks", International Journal of Computers Communications & Control, vol. 12, no. 6, pp:854-870,2017.
[3] Fang W, Zhang W, Chen W, et al. "MSCR: multidimensional secure clustered routing scheme in hierarchical wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, no. 1, pp:1-20,2021.
[4] Harn L, Hsu C, Ruan O, et al. "Novel Design of Secure End-to-End Routing Protocol in Wireless Sensor Networks", Institute of Electrical and Electronics Engineers Sensors Journal, vol. 16, no. 6, pp. 1779-1785,2016.
[5] Bilgin B E, Baktir S, "A light-weight solution for blackhole attacks in wireless sensor networks", Turkish Journal of Electrical Engineering and Computer Sciences, vol. 27, no. 4, pp. 2557-2570, 2019
[6] Liu Y, Dong M, Ota K, et al, "Active Trust: Secure and Trustable Routing in Wireless Sensor Networks", Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2013-2027, 2018.
[7] Rathee M, Kumar S, Gandomi A H, et al. "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks", Institute of Electrical and Electronics Engineers Transactions on Engineering Management, vol. 68, no. 1, pp. 170-182,2019.
[8] Sajan R I, Jasper J,"Trust-based secure routing and the prevention of vampire attack in wireless ad hoc sensor network", International Journal of Communication Systems, vol. 33, no. 8,2020.
[9] X Yu, Li F, Li T, et al. "Trust-based secure directed diffusion routing protocol in WSN", Journal of Ambient Intelligence and Humanized Computing, vol. 2020, no. 5, pp. 1-13,2020.
[10] Aliady W A, Alahmdi S A. "Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks". Institute of Electrical and Electronics Engineers Access, vol. 7, pp. 84132-84141, 2019.
[11] Laxmi B P, Chilambuchelvan A. "GSR: Geographic Secured Routing using SHA-3 algorithm for node and message authentication in wireless sensor networks". Future Generation Computer Systems, vol. 76, pp. 98-105, 2017.
[12] Alromih A, Alrodhaan M, Tian Y, et al. "A Randomized Watermarking Technique for Detecting Malicious Data Injection Attacks in Heterogeneous Wireless Sensor Networks for Internet of Things Applications". Sensors, vol. 18, no. 12, pp. 4346, 2018.
[13] Sarma H K, Kar A, Mall R, et al. "A Hierarchical and Role Based Secure Routing Protocol for Mobile Wireless Sensor Networks". Wireless Personal Communications, vol. 90, no. 3, pp. 1067-1103, 2016.
[14] Selvakumar K, Sairamesh L, Kannan A, et al. "An Intelligent Energy Aware Secured Algorithm for Routing in Wireless Sensor Networks". Wireless Personal Communications, vol. 96, no. 3, pp. 4781-4798, 2017.
[15] Tang J, Liu A, Zhang J, et al. "A Trust-Based Secure Routing Scheme Using the Traceback Approach for Energy-Harvesting Wireless Sensor Networks". Sensors, vol. 18, no. 3, pp. 751, 2018.
[16] Wang Y, Zhang M, Shu W, et al. "An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks". Eurasip Journal on Wireless Communications and Networking, vol. 2018, no. 1, pp.145, 2018.
[17] Devanagavi G D, Nalini N, Biradar R C, et al. "Secured routing in wireless sensor networks using fault-free and trusted nodes". International Journal of Communication Systems, vol. 29, no. 1, pp. 170-193, 2016.
[18] Umar I A, Hanapi Z M, Sali A, et al. "TruFiX: A Configurable Trust-Based Cross-Layer Protocol for Wireless Sensor Networks". IEEE Access, vol. 5, pp. 2550-2562, Mar. 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY