Tnamosn: Trust-Based Neighbor Anonymity in Mobile Opportunistic Social Networks inWsn

Divya.N[1*], R.Muralidharan[2]

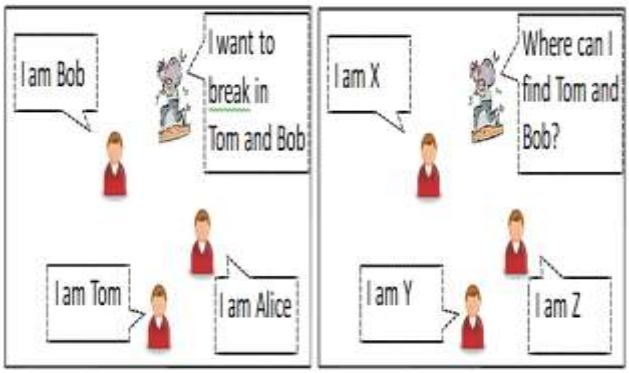
Abstract

Due to the energy constraint of sensor nodes, scalability and network longevity are critical issues for wireless sensor networks (WSNs). Various authentication measures can be used to guarantee the transfer of data between nodes. Authentication is an important protection measure in a sensor network. Making a wireless sensor network safe can be difficult because of its dynamic characteristics. It will unite all networks and take advantage of their strengths to overcome the challenge of user authentication in WSNs. We proposed Trust-Based Neighbor Anonymity in Mobile Opportunistic Social Networks (TNAMOSN), an effective and reliable mechanism for sensor node authentication. Neighbor change does not accept all valid IDs and correct IDs for node anonymity; two discovered identities must provide all manner encryption for mutual identification. We are developing new ideas to allow our "white list" lists to work more quickly and make encountering facts more efficient. The MAC mobility solution provides an authentication sensor to be moved through networks to address the problems associated with authentication. Encryption technologies are used to safeguard the data when moving it through a network. Trust security methods are recommended for use in this document to authenticate a Trusted Certificate. A detailed study and several experiments show the reliability and efficacy of Face Change's operation in Ns2 Simulator.

KeyWords:WSN, MOSNs, Face Change, Trust, Node Anonymity
DOI Number: 10.14704/NQ.2022.20.12.NQ77201 **NeuroQuantology2022;20(12): 2246-2252**

Introduction

There is a high amount of advertising in mobile opportunistic networks (MOSNs) [2] [3] as a sort of late-tolerant networks with the increasing use of mobile devices such as smart phones and tablets (DTNs). When people's mobile devices meet (i.e., are within each other's communication range), they connect. As a result, MOSNs will allow proximity-based social networks without infrastructure because system experience represents the meeting of the people carrying it.Today, the development of the Internet, geographical data networks, and modern consumer technologies has made location-based services successful [4]. Location-based services tend to provide their clients with timely statistical data at the right place to decide [6].The primary task of the WSN network is to generate data and handle those data with traditional storage. But



Potentially infringing on one's privacy. (b) Anonymity of neighbors is the solution

Figure 1: An example of a privacy problem and a potential solution in MOSNs.

WSN generates separate, ordered or unstructured data with new technologies and techniques in various applications [7].

Corresponding author: Divya.N
Address: [1]Assistant Professor, NallamuthuGounder Mahalingam College, Pollachi, [2]Principal, Rathinam College of Arts and

Science, Coimbatore
E-mail: divyanambirajan@gmail.com, rcas.vp@rathinam.in

Because neighboring nodes can directly attach to individual IDs, nodes can readily get reliable ID-based meetings data. When two nodes are within a radius of each other, they are considered neighbours.. However, the explicit use of current IDs creates privacy and security problems by leaking the node ID to neighboring nodes. A malicious node, for example, can first learn the IDs of a certain node. Then, while surrounding nodes interact with real IDs, a malicious node will readily identify targets among neighbours and initiate assaults to damage the system's efficiency or record key records. As seen in Figure 1, (a).

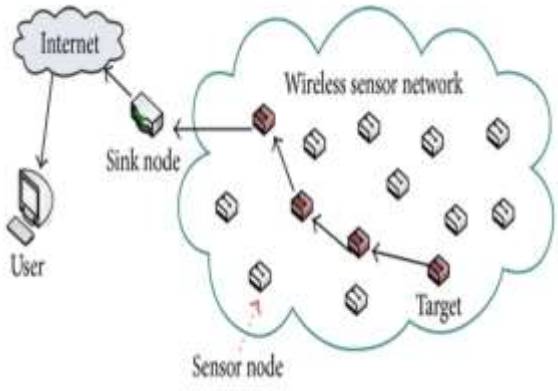


Figure 2: Wireless sensor Network Architecture

Furthermore, malevolent nodes may rapidly discover the meeting of target nodes for assaults if there is no protection. As a result, offering privacy to neighbour nodes is critical in order to prevent the leakage of genuine IDs to neighbours. A permanent handle can't achieve this since it can be attached to a node, allowing hostile nodes to tell the difference between targets and neighbours. Then, as shown in Figure 1 (b), allowing each node to change the nickname used in correspondence with neighbours on a regular basis is an intuitive way to achieve neighbour node confidentiality. However, as neighbor node confidentiality is implemented, nodes cannot gather Valid ID-based knowledge, which disables the MOSN above services. The goal of this study is to lower the amount of energy used by nodes during data transmission. It contributes to increased overall packet transmission to BS by lowering sensor node energy usage. The below is how the article is structured: A survey of the literature on recent studies on routing techniques is included in Section 2. The proposed model is discussed in Section 3. The results and efficiency of the suggested strategy for current algorithms are discussed in Section 4. Finally, Section 5 discussed the conclusion.

Background Study

Some researchers have suggested some localization approaches in recent years to enhance localization protection in various ways. Some of the approaches provide authentication procedures to mitigate the effect of inaccurate location facts. Others, on the other hand, use robust computational algorithms to increase the efficiency of localization schemes. Others, though, propose using the checkpoint system to reduce the effects of attacks.

Daniel D, A., & Roslin, S. E. [2] In WSN, a specification of a trust-based protocol with data validation and honesty checking was forwarded. The sensed data was secured using a mutual symmetric key in this protocol. The encrypted data was signed with a homomorphic MAC tag after fragmentation. After checking the data's correctness and the consistency of each block, the aggregator performs the SUM aggregation process on the signed blocks. The aggregated outcome was sent to the drain, where it checked once more. The procedure was repeated for each sensor based on the sensed effects. Analyzing simulation values reveals that the proposed approach improves data correctness.

Khan, T. et al. [3] the proposed method of massive WSN confidence calculation to enhance collaboration, Reduces resource consumption by providing trustworthiness and protection by detecting hostile (detailed or selfish) sensor nodes. A strong confidence estimation process, assault resilience, and easy trust aggregation at cluster leaders are among the innovative aspects of the proposed scheme (LTS). Data trust, coupled with connectivity trust, is critical in dealing with malicious nodes.

Narayana, K. L. et al. [5] the next neighbor outlier algorithm for identifying dispersed WSNs was suggested. The nearest neighbor is presented and implemented an outliner identification algorithm for distributed WSNs. In this technique, the interval between the measured data is calculated without defects with sensor data.

Sahoo, R. R. et al. [8] the trust-based clustering mechanism for WSNs, which is safe and energy-efficient, offered a practical model of energy consumption. The authors contended that our

energy model is well suited to actual situations since it includes a sensor node's core functions. Clusters closer to the base station are smaller than those further from the base station to balance energy usage between cluster heads; cluster heads closer to the base station will also retain a few energy sources.

Zhang, T. et al. [11] Analysis of the issue of external and internal localization attacks in WSNs, noting that cryptographic systems cannot combat attacks from compromised beacon nodes effectively. The authors have suggested a trust-based protected localization scheme to address this safety issue to pick trustworthy lightning nodes, assess all their identity and behaviors, and use reliable location knowledge to calculate localization performance. The authors have also conducted several simulations to demonstrate that the authors were proposed a scheme that can increase the localization precision for unknown nodes.

Zhao, J. et al. [12] the trust maintenance scheme is an efficient way to detect malicious node misbehavior. A significant range of confidence protection schemes was currently being proposed based on beta delivery. Unfortunately, in the course of node activity, there is a possible hypothesis that two states occur. It may contribute to false confidence values since WSNs have different states. Consequently, it is suggested to create a scheme of confidence and credibility centered on the exponential spread. The exponential distribution in our system is used to express the trust and credibility of nodes. Without taking other states into account, it may create a framework for confidence protection based on good interactions. The trust attribute is redefined since the number of active contacts calculates.

Problem Statement

Face Change will help to identify real IDs anonymously between neighboring nodes and to gather valid ID data. As all nodes disconnect, each node sends encrypted meeting data to the node to collect meeting information. There are a variety of innovative systems in place to protect the findings' confidentiality and uniqueness. Extensive experimental findings show that the present modeling strategy produces scalable network topologies for WSNs and that ROSE will significantly increase the solidity of the network topologies produced by our modeling strategy. ROSE has two phases: the differential grade procedure and the number of edges.

System Model

The proposed work establishes a Trust-Based Neighbor Anonymity in Mobile Opportunistic Social Networks, which allows the sensor node to be authenticated. It also enables a sensor node to switch around several WSNs to address authentication issues. To protecting data when transferring it from one node to another, encryption and decryption techniques are supported. The proposed work employs a confidence protection strategy to include verification via a Trusted Certificate Authority.

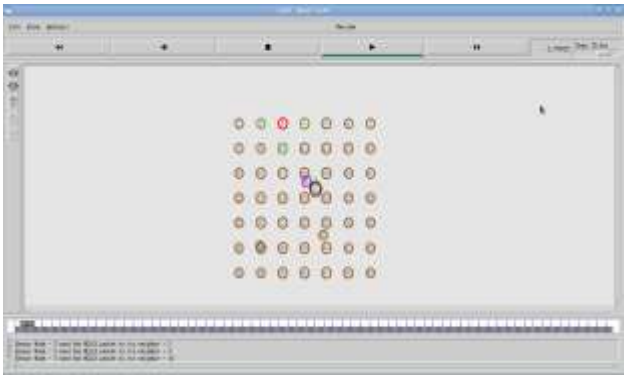


Figure 3: Node Construction

Figure 3 represents Node creation in Ns2 Simulation Tool 0 to 49 sensor nodes

Social Network

The identity of a neighboring node may be deducted easily. In addition to the individual's versatility, mobile devices/nodes migrate across the network. The contact with any node (i.e. device) is minimal. They can only chat if two nodes are interconnected. In this context, a trust authority (TA) is responsible for device administration functions such as system parameter and certificate distribution, as well as attribute authentication (e.g., reputation, membership, ID).There is no way to develop network trust to support applications without a TA. The TA is a dedicated telephone and Internet access server. His genuine ID is also visible for convenient access. Nodes connect to TA in two ways: (1) when they move close to it, and (2) when they are connected to the Internet through LTE. When a node connects to the TA, it can get the most up-to-date system information, such as obtaining legal IDs for surrounding nodes to locate goals. Our priority will be to prevent actual ID leakage during communication with neighboring node and promote information collection.

Cryptographic Techniques are used to selects a security parameter below
Bilinearity
Non-degeneracy
Computability
Commutative Encryption

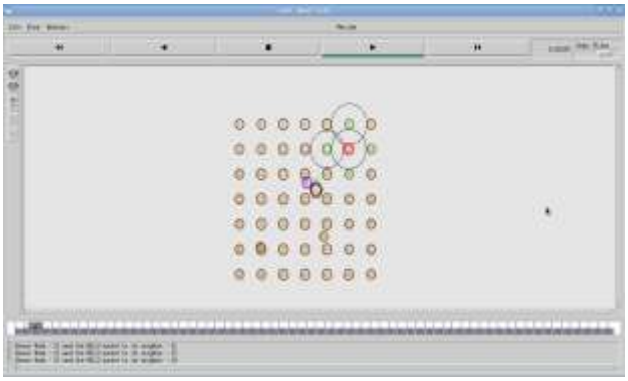


Figure 4: Sending data to Neighbor Node

Figure 4 represents Node 0 considered as Trusted Authority, and Sensor Node 12 sends the Hello Message to its neighbor 11, 13, 19

System Design

The term "anonymity of the neighboring node" applies to the idea that each node does not recognize its neighbors' exact identification. This is achieved by enabling each node to communicate secretly with the neighboring nodes. When a node separates from a next node, all communication layers and communication parameters are switched to random pseudonyms.
This solution has several issues when it comes to the processing of knowledge. First, the proof must be secured from contamination and manufacture during the routing. Secondly, the proof must be collected successfully and clearly. Finally, based on its trust in the node, a node may wish to exert control over the evidence's contents. Securing the safety of data retrieval ensures; face Change addresses this issue by using bilinear links to generate encryption key, code and promises evidence relay retrieval. The recipient node defines a relay node during the meeting, and its real ID is encrypted with a public key, and this information is delivered to the evidence manufacturer. After disconnecting the two nodes, the creator sends the proof to the relay node, which decrypts the receiver node's actual ID before sending it to the receiver node.

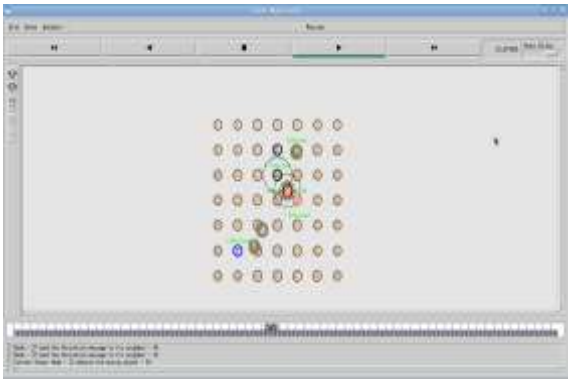


Figure 5: Detecting Moving object

Figure 5 represents the Node 27 send activation message to its neighbor 34 and current sensor node 12 detects the moving object

Algorithm 1: MOSN routing algorithm steps:

```
Procedure ENCOUNTERNODE(Mi)
exchangeCentralityValues()
exchangeOnlineContactsLists()
exchangeInterestNodeList()
exchangeForwardingHistroyList()
do m inmessage buffer for everymessage
        D←m.destination()
        myMLS←computeMLScore()
        encounterMLS←computePeerMLScore()
        if encounter MLS ≥ my MLS|| Mi==D then
                forwardMessage(m, Mi)
        end if
end for
for every message m in the forwarding history table
_list do
if timestamp > last encounter with Mi
&&IfmsgsourceID equals myID
        if last encounter with forward ID > last
encounter with Mi
&&forwarderID.receivedMessage(msgID) == false
then
        ESS ← forwarderID.selfishScore()
        forwarderID.setSelfishScore(ESS+1)
        end if
end if
end for
end procedure
```

Algorithm 2: Polynomial-time algorithm step:

```
T1 = (1, {(1, , 1, )})
α(T1) = 0
T1 = { T1 }, ∀j ∈ {2 . . . n}, Tj = ∅
for j = 1, . . . , n − 1
        for each state T ∈ Tj
 for each Δ ∈ δ(T)
```

T ' = τ(T, Δ)
if valid(T ') = FALSE: continue
score = α(T) + score(Δ)
Define t to be the integer such that
T '= (t, {σ1 . . . σr})
if T ' ∈ Tt
Tt = Tt ∪ { T '}
α(T ') = score
bp(T ') = (Δ)
else if score >α(T ')
α(T ') = score
bp(T ') = (Δ)

Algorithm 3: Data and ID matching algorithm
for each time slot 1 ≤ t ≤ |T| do
NeighborNode ID(t) ← The set of nodes whose transmission range covers the sink trajectory at t
for each sensor s Є NeighborNode ID (t) do
Data ID (s) ←
energy budget(s)+harvestedEnergy
end for
eligibleNodes (t) ← The set of nodes from Neighbor(t) which satisfy constraint
for each sensor s' Є eligibleNodes(t) do
Compute Throughput(s')
end for
sselect ← arg max eligibleNodes(t) = = f{Throughput(s)}
Allocate timeslot t to sselect
Update energy budget of sselect
overallThroughput ←
overallThroughput + Throughput(sselect)
end for
return overallThroughput

Advanced Extensions

Face Change has given direct Anonymity to neighbors at the expense of indirect encounter knowledge collection. They often see that an individual has a few trustworthy peers and can share the true identity. Neighbor identity must also be preserved for nodes to identify responsible nodes anonymously. Therefore, nodes may find trusted nodes in an anonymous manner. Second, we must ensure that when eavesdropped, two nodes that trust each other will surreptitiously swap their real identities.

Creating the White List

To label trustworthy nodes, we use a token-based scheme. As two nodes decide that they are responsible, they alert the TA of their partnership. The TA then produces a token that has never been seen before at random.

Finding Trusted Nodes

When two nodes first connect to see if the "white list" functions is available. If they don't, they go through the required Face Change for encountering the knowledge set. If so, they use the commutative encryption algorithm to determine if they trust each other anonymously.

The exchange between Trusted Nodes

After deciding their trustworthiness, they will exchange their real IDs during the encounter. Therefore, they cannot deal explicitly with the plain text since we expect the presence of eavesdroppers.

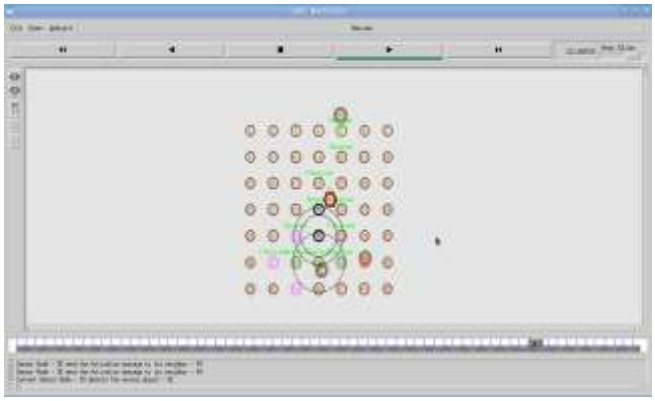


Figure 6: Neighbor Discover with moving object

Figure 6 represents the moving objects are detected while the sensor node activating to its neighbor nodes

Security Analysis

A modern scheme called the "white list" would not affect the confidentiality of nodes or make them traceable. To begin with, all tokens are encrypted with a single key before being transferred to the other node when two nodes check their trust. The result is, each node tokens will not be revealed to other nodes, and malicious nodes will not recognize other nodes' tokens and declare unreliable connections. The key for encrypting tokens is given randomly for each experience.

Evidence Finding Relaying

The group-oriented routing effectiveness of the MOSN routing algorithm is demonstrated from the originator to the relief node and from the relay node to the recipient. This kind of routing strategy

means that groups were built based on record nodes. Nodes inside a network have a higher opportunity than nodes from other communities to access each other. This first involves sending a packet to the community containing the destination node and then routing it to the destination node via an intra-community transmission.

Figure 7: Calculate the next location of the moving object

Figure 7 represents the current sensor node 41 calculated the next location of the moving object to 52.

Discussion

The simulation platform used in this proposed protocol is NS2. The Nodes are Created 0 to 49. The results are compared with existing methodologies like Packet Delivery Ratio, Energy Consumption, Packet Loss, and Throughput.

Figure 8: Packet Delivery ratio comparison

Figure 8 represents the existing and proposed comparison chart for packet delivery ratio. In X-axis denotes Time and Y-axis denotes the PDR.

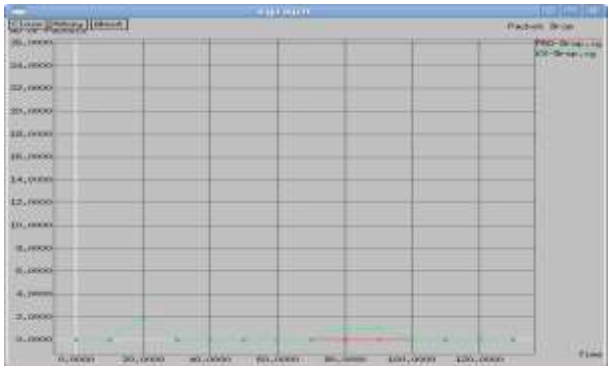


Figure 9: Packet Drop comparison

Figure 9 represents the packet drop comparison chart. In X-axis denotes Time and Y-axis denotes the No of Packets.

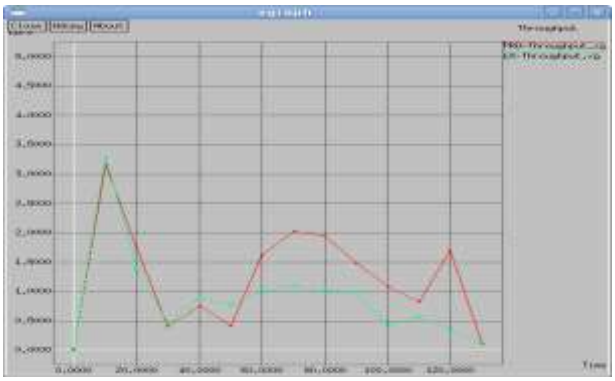


Figure 10: Throughput Comparison

Figure 10 represents the comparison for Throughput. In X-Axis denotes the Time and Y-Axis Denotes the PDR.

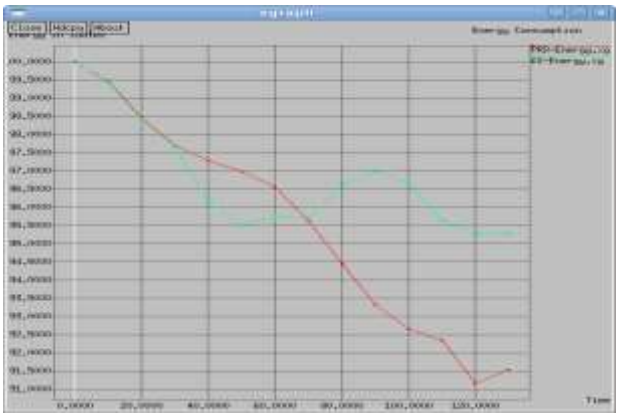


Figure 11: Energy Comparison Chart

Figure 11 represents the Energy Consumption comparison chart. In X-axis denotes the time, and Y-axis denotes the Energy Levels.

Conclusion

The approach Trust-Based Neighbor Anonymity in

Mobile Opportunistic Social Networks (TNAMOSN), which guarantees the security of data in Sensor Networks when sent from one node to another neighbor node, was implemented in the suggested work. Authentication is a fast and stable mechanism for authenticating a sensor node using a data ID. It also enables a sensor node to switch around several WSNs to address authentication issues. Integrating WSNs is a technique for analyzing cell network protection problems. They should merge all networks to maximize their capacities, resolve protection problems, and address the authentication problem in WSNs. The proposed work incorporates the idea of Trusted Certificate Authority, which solves confidence between nodes by creating certificates and signatures. Interesting problems in future work on the construction of a robust reputation system include exact and efficient modeling of confidence/reputation and management of environments in wireless sensor networks, the extent of the collaborative compliance examined for the network's success, the provision of overhead communication and the time required for accurate reputation.

References

Chen, K., & Shen, H. (2015). Fine-Grained Encountering Information Collection under Neighbor Anonymity in Mobile Opportunistic Social Networks. 2015 IEEE 23rd International Conference on Network Protocols (ICNP). doi:10.1109/icnp.2015.25

Daniel D, A., & Roslin, S. E. (2020). Data validation and integrity verification for trust-based data aggregation protocol in WSN. Microprocessors and Microsystems, 103354. doi:10.1016/j.micpro.2020.103354

Khan, T., Singh, K., Son, L. H., Abdel-Basset, M., Long, H. V., Singh, S. P., &Manjul, M. (2019). A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks. IEEE Access, 1–1. doi:10.1109/access.2019.2914769

Maheshwari, P., Sharma, A. K., & Verma, K. (2020). Energy-Efficient Cluster based Routing Protocol for WSN using Butterfly Optimization Algorithm and Ant Colony Optimization. Ad Hoc Networks, 102317. doi:10.1016/j.adhoc.2020.102317

Narayana, K. L., Gouda, B. S., Mishra, T. K., & Sethi, N. (2020). Nearest Neighbor outlier detection Algorithm for Distributed WSN. 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA). doi:10.1109/iccsea49143.2020.9132870

Padmapriya, K., & Sridhar, S. (2014). An efficient localization for wireless sensor network using nearest neighbor reference method. International Conference on Information Communication and Embedded Systems (ICICES2014). doi:10.1109/icices.2014.7033840

Singh, V. P., Hussain, M., & Raina, C. K. (2016). Authentication of base station by HDFS using trust based model in WSN. 2016 International Conference on Communication and Electronics Systems (ICCES). doi:10.1109/cesys.2016.7889844

Sahoo, R. R., Singh, M., Sardar, A. R., Mohapatra, S., & Sarkar, S. K. (2013). TREE-CR: Trust based secure and energy efficient clustering in WSN. 2013 IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN). doi:10.1109/ice-ccn.2013.6528557

Yan, A., & Wang, B. (2017). An adaptive WSN clustering scheme based on neighborhood energy level. 2017 IEEE 3rd Information Technology and Mechatronics Engineering Conference (ITOEC). doi:10.1109/itoec.2017.8122540

Zhang, Y., & Yuan, X. (2016). Fault diagnosis in clustering WSN based on neighbor cooperation. 2016 Chinese Control and Decision Conference (CCDC). doi:10.1109/ccdc.2016.7531274

Zhang, T., He, J., & Zhang, Y. (2011). Trust Based Secure Localization in Wireless Sensor Networks. 2011 2nd International Symposium on Intelligence Information Processing and Trusted Computing. doi:10.1109/iptc.2011.21

Zhao, J., Huang, J., &Xiong, N. (2019). An Effective Exponential-based Trust and Reputation Evaluation System in Wireless Sensor Networks. IEEE Access, 1–1. doi:10.1109/access.2019.2904544