ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2019.0304

DETECTION OF MALICIOUS NODES IN WIRELESS SENSOR NETWORK

M. Babu[1], M. Ramkumar[2] and M. Shenbagapriya[3]

[1,2]Department of Computer Science and Engineering, Gnanamani College of Technology, India

[3]Department of Electronics and Communication Engineering, Sri Satya Sai University of Technology, India

Abstract

Wireless Sensor Network (WSN) can be used as an important concept to reduce the redundancy and energy consumption. To optimize the wireless sensor networks for secured data transmission both at cluster head and base station, data aggregation is needed. The existence time of sensor network diminishes due to energy inefficient nodes for data aggregation. Henceforth aggregation process in WSN ought to be advanced in energy efficient way. Data aggregation is performed in every router while forwarding data. It is difficult to identify and isolate the compromised nodes so as to abstain from being deceived by the distorted data infused by the enemy through compromised nodes. In any case, it is trying to secure the flat topology network effectively in light of the poor adaptability and high communication overhead. We discuss a mechanism that distinguishes malicious nodes by the collaboration of appropriate nodes and logically isolates the recognized, malicious nodes from remote sensor systems. Also this paper describes about the attacks and security goals in the WSN.

Keywords:

Wireless Sensor Network, Data Aggregation, Malicious Node, Security Goals

1. INTRODUCTION

The WSN comprises of a sensor nodes that are battery controlled and are equipped with incorporated sensors, a data-processing unit, a small storage memory, and short-range radio communication. Commonly, these sensors are randomly deployed on the field. Wireless sensor networks comprise of numerous smaller devices, consist of sensor nodes for some applications like acoustic, seismic and image sensors form a wireless network. Every sensor node in the system collects data from the environment, and sends the detected information to a base station, either from sensor node to sensor node under multi-hop, or specifically to a base station under single-hop information communication [3] [4].

WSN can collect data where it is embedded from the environment. The data are normally processed first by the sensor nodes, then sent to the sink node for further processing through unknown channels. Sensor network uses include environmental protection, traffic control, public safety, medical, home and workplace security, transport and battlefield tracking. Such systems are likely to be attacked because of their criticality [9].

A WSN can be attacked in several ways. Of example, during transit you will spot different fields of a message so that it is a changed copy of the original message that the receiver is getting. A node (hardware and/or software) can also be exploited to modify its behaviour. Various attack types require various counter-measures [9].

The inherent safety problems may impede the growing value of sensor networks. It technique is closely linked to the field of fitness. The nodes are therefore as open as the governing case. Everybody can still use the cellular link used in communications. In terms of computer power, memory, bandwidth and battery power, the nodes are also highly restricted. Any malicious adversary may therefore launch a set of attacks which could partially or totally render the network useless.

A collection of safety primitives that can boost the robustness and stability of the network should be included in order to resolve the security problems present in WSN. For example, the creation of secure communication channels requires encryption primitives and key management systems must be used for the distribution of the security credentials used for those primitives. Additional services should also be in operation, such as self-healing and confidence management. You may help protect the core network protocols: replication, time syncing and routing. Finally, if a sensor network includes certain things such as distributed computing, a safe location, and a mobile base station position [10].

Trust evaluation helps to enhance WSN health. For e.g., sensor nodes may need to know which other nodes you trust to forward a packet for the routing phase. A node may have to trust other neighboring nodes to monitor anomalous measurements for sensing purposes. Others include data divulgation results and core interchange confidence in sensor networks. Since the sensor nodes are usually restricted devices, confidence management systems must be light enough to deliver good performance without compromising the system functionality. Therefore, because of the centralized existence of those networks, their trust management systems can be targeted [10].

1.1 SUITABILITY OF TRUST

Given the above attacks that can affect WSN functionality, it can be argued that the adoption of WSN trust management system does not bring sufficient benefits. However, as we will see here, trust is an important tool for addressing one of the fundamental issues facing WSN: the problem of collaborative uncertainty. Additionally, confidence generated between nodes can be used outside cooperation for other purposes. In fact, if future attacks on a confidence management system are identified, more reliable solutions should be developed.

Because of these advantages, confidence protection is not just a basic element that allows a fully operational wireless sensor network to be created. It should also be pointed out that. For instance, existing industry sensor network guidelines and requirements do not describe trust (for the actions of other nodes) as one of their points. Nonetheless, as mentioned in this section, confidence management is an important component of a sensor network security architecture because it can solve problems and, when used appropriately, it can have other useful benefits.

We will begin with the concept of collaboration to explain the appropriateness of confidence for sensor networks. In order to provide the network services, all WSN members (sensor nodes and base stations) need to collaborate. Sensing and routing are examples of such cooperation processes. To receive spatial knowledge from the world, all sensor nodes use their sensing hardware.

As many sensors can be mounted in a small area, the data provided by those sensors can be aggregated if the network consumer is interested in a general environment summary only. In turn, each node serves as a router that passes physical information from other nodes to the base station. Nodes can choose whether to prioritize speed over energy by sending the information via both the fastest link and the less energy consuming nodes.

A node will figure out which nodes are more likely to carry out a particular task in order to ensure effective cooperation. If a node understands in advance how the different network components respond in any situation, a perfect decision may be made. But in a WSN it is difficult to clearly establish or guarantee the outcome of a particular situation. In other terms, we will take account of ambiguity.

The main source of uncertainty is information asymmetry (a partner does not have all the information it needs) and opportunism (the partners involved have different objectives). No issue with sensor networks where no node maliciously behaves opportunism: all members of the network operate towards a common goal and have no reason or desire to act selfishly. The asymmetry of knowledge, though, could be a concern because a sensor node may fail or the state of the atmosphere can shift (for example, the wireless channel). In addition, if subverted nodes operate inside a WSN, asymmetry and opportunism of information must be taken into account. A node can therefore not realize how a business partner should act in advance.

Confidence management systems provide a successful solution to the uncertainty problem. Although the future cannot be understood right, the past behavior of nodes are expressed in the ideals of integrity and confidence. When a node has been successful in carrying out a certain task in the past, the same task is assumed to be reliable in the future. A co-operative mechanism with the most stable nodes could thus begin a node. The underlying WSN trust management system helps to detect defective and malicious nodes.

The main purpose of using WSN trust is closely linked to self-sufficiency: a wireless sensor network should not only be able to configure itself during normal network operations but also in exceptional cases. With knowledge of the reputation and actual behaviour, nodes can take appropriate steps when making operational decisions (knowing the best partner to start a cooperation) or in extreme situations.

Self-authentication is not the only aspect that trust will benefit: a trust management system can also endorse and/or use other security protocols and procedures (e.g. device safety, IDS, key management, confidentiality). As far as hardware protection is concerned, existing codes and certificate systems can be integrated as tools for testing the integrity of untrusted nodes into a trust management system without any difficulty.

In addition, complex services such as secure location and intrusion detection systems may benefit from the existence of a trust administration system through the use of the system's output as a decision-making aid or through the provision of useful confidence input that could be helpful for any other service.

In addition, the sensor networks can use the confidence to monitor data disclosure: the trust given to each data complainant can be used to evaluate if data are revealed or if only a sample of data is released or if the request is rejected [10].

2. RELATED WORK

Wireless sensor network are frequently deployed in an antagonistic condition and work without human supervision, singular node could be effectively imperiled by the enemy because of the requirements, for example, battery lifetime, smaller memory space and constrained processing capacity. Security in WSN has been a standout amongst the most vital subjects in the WSN research network.

The work reported by Zhou [2] is closest to our approach. They proposed a novel weighted-trust evaluation based plan to distinguish compromised or gotten misbehaved nodes in wireless sensor systems. The fundamental thought is that Forwarding node give trust esteems to every one of the nodes in the group if a node sends wrong data which suggests that a node has been endangered or out is of function, the Forwarding node straightforwardly brings down that node's trust level.

Eiji et al. [1] suggested cooperative detection and an isolation mechanism to secure the dependability of a remote sensor network, regardless of whether malevolent nodes with a stolen shared key development in a network’s route, mechanism completely discards the distinguished, falsified malevolent nodes from the systems.

The work shown in [3] are Security goals for WSN, application layer attacks, summary of attacks against the sensor network routing protocols.

3. SECURITY GOALS FOR WIRELESS SENSOR NETWORKS

In the application layer, the sort of attack is subversion and malicious nodes. Counter measure of that is malicious node identification and isolation. In network layer, the kind of attack is wormholes, sinkholes, Sybil, countermeasure of the key management, secure routing. In data link layer, the attack type is layer encryption. In physical layer, the type of attack is dos and node. Counter measure is adaptive receiving wires, spread spectrum [6].

3.1 PHYSICAL ATTACKS

In a physical attack, the attacker gains guide access to the figuring gadget equipment. This makes a refusal of-benefit attack effectively conceivable: the assailant can just pulverize the sensor nodes. Physical access likewise permits him to get to a node's segments with no software layer included. This is as opposed to a remote attack, where the attacked PC is gotten to through some convention or application layer, which gives it the likelihood (at least, in principle) to identify the attack and respond appropriately. In a physical attack, this kind of self-surveillance is not accessible to the device under attack and would just be conceivable by extra measures, for example, outer observation. This makes a physical attack extremely powerful.

3.2 INTERFACE ATTACKS

Interface attacks misuse vulnerabilities of the interfaces a device gives so as to enable access to its very own services or to get to outside services. For remote correspondence interfaces, there are evident attacks, for example, eavesdropping, jamming, traffic analysis, and message injection among others. They are encouraged by the broadcast nature of remote communication, and the way that gets to is effectively conceivable without the risk of detection. A review can be found, e.g., in. Interface attacks can likewise be executed on the level of a service API, for instance, those of security processors. Here, substantial directions are executed in strange succession, subsequently inciting unintended conduct for the attacker. To our insight, the service (message) interfaces of sensor systems have not been examined with respect to security vulnerabilities.

3.3 SOFTWARE-LEVEL ATTACKS

A powerful attack is the infusion of code into an execution condition since this yields conceivably full authority over this condition. Such attacks are basic in the Internet world, where ineffectively administrated hosts are helpless to the antagonistic remote control. One reason for this is code portability for example code is frequently downloaded from remote destinations and locally executed. Regardless of whether systems for code affirmation exist, these are frequently bypassed by social designing or client carelessness. Sensor systems are nearly more closed environments, however, code refreshing is a typical element, but that presents comparable vulnerabilities.

4. STUDY ON MALICIOUS NODE DETECTION

In this paper, to protect data reliability in wireless sensor networks, we propose cooperative-based falsification detection and an isolation mechanism for the malicious nodes detection and also introduced weighted-trust evaluation based method to detect malicious nodes in WSN.

4.1 WEIGHTED TRUST ELEVATION (WTE) TECHNOLOGY

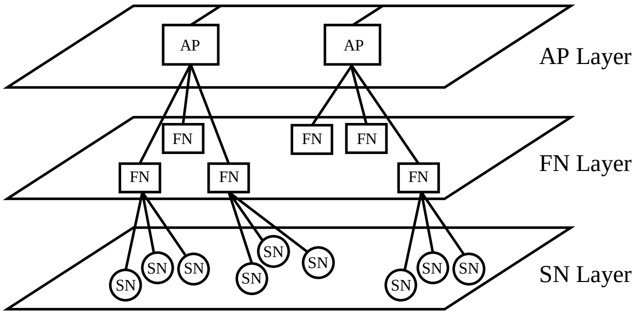
4.1.1 System Architecture:

The Fig.1 exhibits the system design in which our weighted-trust assessment conspire is executed. It is a three-layer progressive system engineering, which comprises of three kinds of sensor nodes similar to the architecture utilized in [2] [5]:

- Low power - Sensor nodes
- Higher-power - Forwarding Nodes
- Access Points (*AP*) or Base Stations (*BS*).

In contrast to sensor nodes in the level sensor networks, sensor nodes in the lowest layer of the hierarchical network does not offer multi-hop steering capacity to its neighbour.

Various Sensor Nodes (*SN*s) are composed as a gathering and controlled by a higher layer node, the Forwarding Node (*FN*). Along these lines, every sensor node just speaks with its *FN* and gives data, for example, sensor perusing to its *FN*. *FN*s are situated on the second layer on the sensor node layer and offers multi-hop routing capacity to *SN*s or different *FN*s. We expect the *FN*s are trustful and won't be endangered. We likewise expect the *AP*s are trustful, generally, the foe can infuse any information without been identified.



The Fig.1. Architecture of the hierarchical WSN

Each *FN* has two remote interfaces, one imparts with lower layer nodes (*SN*s), which have a place with it is the board and alternate interfaces with higher layer nodes-Access Points (*AP*s).

The *AP*s are situated on the most elevated layer in a wireless network and have both wireless and wired interfaces. *AP*s give multi-hop routing for packets from *SN*s and *FN*s inside radio range, notwithstanding routing information to wired systems. *AP*s likewise have the usefulness of sending control data from wired systems to *FN*s and *SN*s

This various levelled system can likewise be considered as an appropriated data accumulation framework. *SN*s assemble data and report to its *FN*. In light of the data gathered from *SN*s, *FN*s register the accumulation result and submit the data to *AP*s. Nonetheless, since *SN*s might be bargained and report counterfeit data, it is critical for *FN*s to confirm the accuracy of the data gathered from *SN*s. Thus, it is likewise wanted that *AP*s have the capacity of confirming the committed information. The Table.1 outlines the emblematic documentation utilized all through this paper.

Table.1. Symbolic notations

Symbol	Meaning
SN	Sensor Node
FN	Forwarding node
AP	Access point
BS	Base station
W_n	Weight range
E	Aggregation result
U_n	Sensor node output

4.1.2 Malicious Nodes Detection using Weighted Trust Evolution Technique:

As shown before, sensor nodes in sensor networks are normally conveyed in threatening conditions, for example, war zones. Thus, a sensor node might be traded off or out of capacity and after that gives off-base data that may misdirect the entire system. This issue is called as the Byzantine issue. For instance, a compromised sensor node (malicious node) can always report mistaken data to higher layers. The aggregator (*FN* or *AP*) in the higher layer may make a wrong aggregation result because of the impact of the effect of the malicious node. So an essential issue in sensor systems to identify malevolent nodes disregarding such Byzantine issue. As the initial move toward the solution for the issue, we demonstrate it into a load based system has appeared in Fig.2. The system is adjusted in the design between a gathering of sensor nodes and their sending nodes.

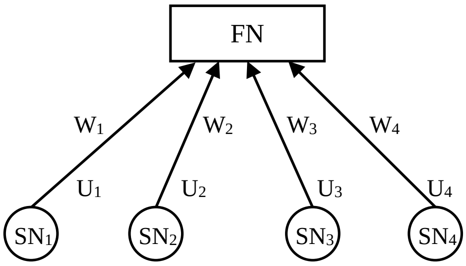


Fig.2. Weight based network for hierarchical sensor network

As appeared in the figure, a load *W* is allocated to every sensor node. The *FN* gathers all data given by *SN*s and computes an accumulation result utilizing the load appointed to every *SN*:

$$E = \sum_{n=1}^{N} W_n U_n \tag{1}$$

where, E is the aggregation result and W_n is the load extending from 0 to 1. A fundamental concern is about the meaning of sensor node's output U_n. In practice, the output information U_n may be false or true information or continues numbers such as temperature reading. In this manner, the definition of output U_n is usually depending on the application where the sensor network is used.

The accompanying issue is to refresh the weight of each sensor node dependent on the rightness of data reported. Refreshing the weight of every sensor node has two purposes. First, if a sensor node is imperiled (turns into a malevolent node) and oftentimes sends its report conflicting with the final conclusion, its weight is probably going to be diminished. At that point, if a sensor node's weight is lower than a particular limit, we can distinguish it as a malicious node. Second, the load likewise chooses how much a report may add to the final choice. This is sensible since if the report from a sensor node tends to be incorrect, it should be counted less in the final decision.

This identification method can be broadly utilized in various type of sensor systems. For instance, the number of sensor nodes can vary in the method, which makes it appropriate for large and small systems. Notwithstanding, the depiction of sensor node yield and an updating scaling factor which are reliant on the connected application require to be resolved cautiously so as to accomplish proficient and high precision location

4.2 COOPERATIVE DETECTION FOR FALSIFICATION AND ISOLATION OF MALICIOUS NODES

The definition of sensor nodes are defined as follows:

- **Proper Node**: a node at the initial configuration on the network that can transmit both the original packet and forward other packets.
- **Cooperative Node**: a proper node that is also a common neighbour node of two successive nodes in a route.
- **Monitoring Node**: a new-entry node and a re-entry node to a network. It can forward a packet, but is not permitted to transmit the original packet.
- **Malicious Node**: A node with a stolen imparted key to which it can adulterate packets and cover distortion by different pernicious nodes.
- **Isolation Node**: a node through which falsification is detected by proper nodes.

4.3 COOPERATIVE DETECTION FOR FALSIFICATION

Cooperative detection for falsification is performed [8] as it were by a legitimate node sending packet yet in addition by different cooperative nodes. In Fig.3, the fundamental cooperative detection for falsification is shown. Nodes A, C, D and E are proper for falsification is appeared. Nodes A, C, D and E are legitimate nodes, and node B is a malicious node with a stolen shared key. Nodes A, B, and C are progressive nodes in a course, what's more, nodes D and E are a basic neighbor of nodes A and B; that is, and nodes D and E are cooperative nodes. Every packet sent from a node includes a MAC value generated by a shared key. At the point when node B distorts a packet from node An and advances it to node C, node C does not think about the misrepresentation since node B connected a legitimate MAC incentive to the packet utilizing the stolen shared key.

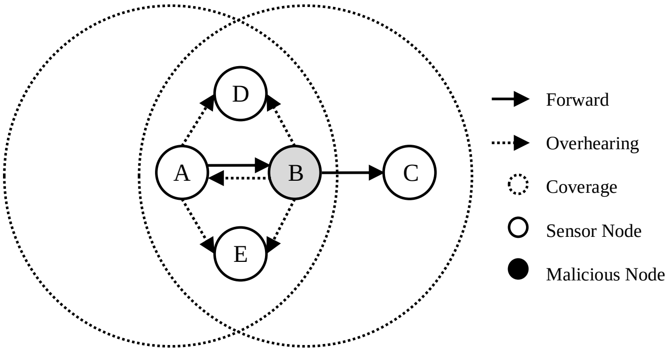


Fig.3. Cooperative detection for falsification

In any case, node A can identify node B falsification since it can think about its unique information in a packet sent to node B with the information in the bundle sent by node B, as the watchdog mechanism. Nodes D and E can likewise recognize the distortion since they can catch the packet sent from the two nodes A and B. In this way, nodes D and E can look at the information in the packet sent by the two nodes A and B and decide if the information has been falsified.

5. RESULTS AND DISCUSSIONS

The Fig.4 demonstrates the flow of isolation. At the point when a node recognizes falsification by another node, the identifying node communicates a detachment report that distinguishes the node distorting a packet as malevolent and informs its neighbors. If the node falsifying is a neighbor node to the node that gets the isolation report, it advances the report and continues to the isolation process, and the other accepting nodes discard the isolation report. The isolation report is sent to the majority of the neighbors of the falsifying node with low traffic [7].

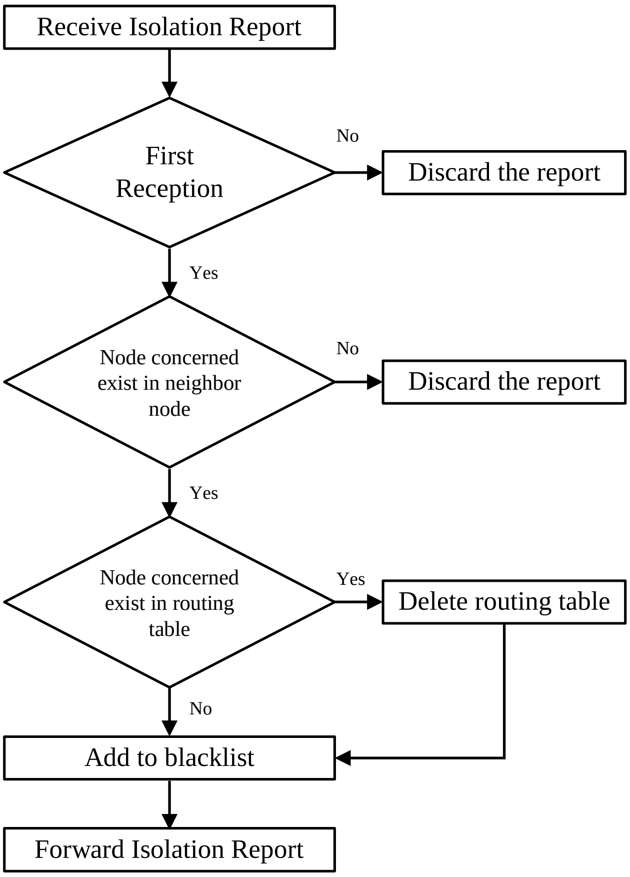


Fig.4. Isolation flowchart

This isolation procedure is performed by all the falsifying node's neighbors since they received its isolation report. The procedure is made out of two cases. Whenever the falsifying node is incorporated into the routing table of the processing node, its entrance is erased from the routing table and entered on a node blacklist. Since the cancellation totally takes out the course to the falsifying node from its neighbors, the distorting node is sensibly detached from the system.

At the point when the falsifying node is excluded in the routing table of the nodes, it is entered on a blacklist, which restricts reentry to the system by the separated malicious node. The node disposes of a route request for from a node on its blacklist. In the event that a segregated vindictive node sends a route request for, it is received by the majority of its neighbors. The blacklist of every one of its neighbors definitely incorporates the asked disconnected node as the aftereffect of the isolation process, and the isolated node request is discarded by its neighbors and it cannot re-enter the network.

The proposed WTE detection system is implemented in NS-2 simulator. The sensor nodes are deployed randomly in an area of 200×200m^2. Simulations were performed for network size of 60 - 200 nodes in steps of 20. For each scale of the network, the detection performance of the proposed IDS is addressed at 100 round tests. The degree of identification of the proposed IDS is equivalent to 23, 24 and 25.

The Fig.5 shows that a distinct confidence factor from those measured nodes, the WTE average detection rate of proposed WTE is 0.8, which is higher than the detection rate of 23, 24 and 25. The network not only relies on the credibility of the system but also takes into account the values of its actual confidence measured.

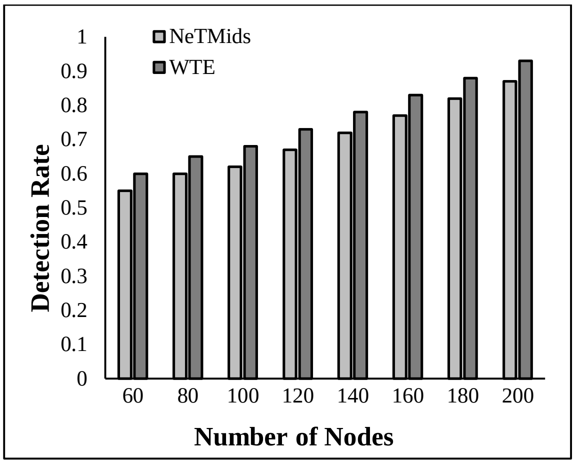


Fig.5(a). Detection rate without cooperative detection

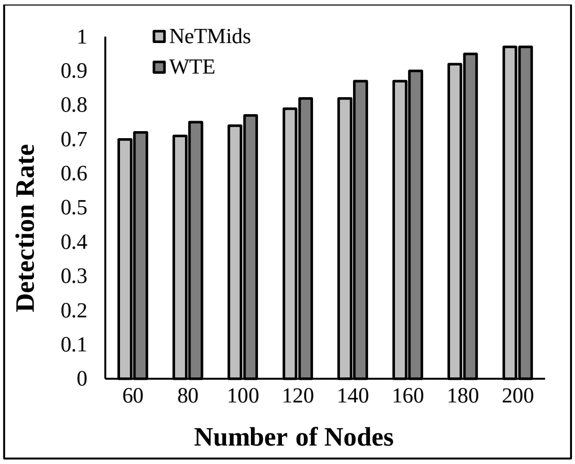


Fig.5(b). Detection rate with cooperative detection

6. CONCLUSION

This study presents a novel weighted-trust evaluation based method to detect malicious nodes in wireless sensor networks. Also describes the attacks and security goals in the wireless sensor network, cooperative detection techniques for falsification, isolation of malicious nodes are explained. The aggregation process in WSN is operated in energy efficient way.

Data aggregation is performed in every router while forwarding data. It is difficult to identify and isolate the compromised nodes so as to abstain from being deceived by the distorted data infused by the enemy through compromised nodes. In any case, it is trying to secure the flat topology network effectively in light of the poor adaptability and high communication overhead.

REFERENCES

[1] Eiji Nii, Takamasa Kitanouma, Naotoshi Adachi and Yasuhisa Takizawa, "Cooperative Detection for Falsification and Isolation of Malicious Nodes for Wireless

Sensor Networks in Open Environment", *Proceedings of 7th Asia Pacific IEEE Conference on Microwave*, pp. 1-8, 2017.

[2] V. Porkodi, A.S. Mohammed, V. Manikandan, "Retransmission DBTMA Protocol with Fast Retransmission Strategy to Improve the Performance of MANETs", *IEEE Access*, Vol. 7, pp. 85098-85109, 2019.

[3] P. Padmaja and G.V. Marutheswar, "Detection of Malicious Node in Wireless Sensor Network", *Proceedings of IEEE 7th International Conference on Advance Computing*, pp. 1-7, 2017.

[4] A.S. Mohammed and V. Porkodi, "Improved Enhanced Dbtma with Contention-Aware Admission Control to Improve the Network Performance in Manets", *CMC Techscience Journal*, Vol. 6, No. 2, pp. 435-454, 2019.

[5] C. Karlof, N. Sastry and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", *Proceedings of 2nd International Conference on Embedded Networked Sensor Systems*, pp. 1-5, 2004.

[6] S. Roy, M. Conti, S. Setia and S. Jajoida, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 4, pp. 681-694, 2014.

[7] W.R. Pires, T.H. De Figueiredo, H.C. Wong and A.A.F. Lourerio, "Malicious node detection in wireless sensor networks", *Proceedings of IEEE 18th International Symposium on Parallel and Distributed Processing*, pp. 26-30, 2004.

[8] B. Rajasekaran and C. Arun, "Detection of Malicious Nodes in Wireless Sensor Networks based on Features using Neural Network Computing Approach", *International Journal of Recent Technology and Engineering*, Vol. 7, No. 4, pp. 188-192, 2018.

[9] H. Yang and F. Cheng, "A Novel Wireless Sensor Networks Malicious Node Detection Method", *Proceedings of International Conference on Security and Privacy in New Computing Environments,* pp. 697-706, 2019.

[10] J. Lopez, R. Roman, I. Agudo and C. Fernandez-Gago, "Trust Management Systems for Wireless Sensor Networks: Best Practices", *Computer Communications*, Vol. 33, No. 9, pp. 1086-1093, 2010.