DOI: 10.21917/ijct.2021.0382

ENERGY EFFICIENT BASED SECURE DATA TRANSMISSION FOR MULTI HOP TRUST MANAGEMENT TECHNIQUE USING WIRELESS SENSOR NETWORK

S. Gayathri and A. Senthilkumar

Department of Computer Science, Arignar Anna Government Arts College, India

Abstract

Secure data transfer is intended to keep data safe from illegal access, damage, or disruption. In this proposed technique, an intrusion prevention system is built to counter the rapidly growing threats offered by the current generation of malware, software, and exploits. As the number of intruders has grown, the network environment has become more complicated, making threat mitigation more difficult. Modern wireless sensor networks have emerged for the aim of transmitting important information and services to an ever-growing set of users. Security is the most important issues in wireless network. Using this proposed Multi Hop Trust Management (MHTM) approach; trust management technique is used to identify the trusted nodes with malicious node. Then secured and efficient way of data transmission are directed and communicated to any kind of networks re confirmed here. The result attained shows MHTM technique attains better performance than TSRP in stipulations of energy efficiency, data transmission delay, communication overhead, throughput, malicious sensor device misclassification rate and identification.

Keywords:

Wireless Sensor Network, Cluster Heads (CH), Cluster Member (CM), Malicious Nodes Identification (MNI) and Security.

1. INTRODUCTION

A discrete network with a large number of network nodes that are all autonomous and modest in size is termed as wireless sensor network. It includes a huge spatially dispersed sensors, and networks assist sensor nodes in collecting data, then processing the data with routing protocol to communicate data to base station, and they form a connection with one another in a different type of topology to record best results [1].

The primary goal of a WSN network is to gather information and sense information samples in a certain region and communicate these readings to BS. Sensor networks feature one or more centralized control points known as Base Stations. Because the sensor nodes are spread out across a broad region, they are unable to interact directly with the BS. Packets are sent from the source to the base station via routing procedures. These routing protocols, on the other hand, must ensure that packets are delivered in a secure way, guaranteeing that neither adversary nor unauthentic individual has access to the information be sent [2].

Environmental monitoring, smart home and industrial production, as well as military and medical applications, have all benefited from wireless sensor networks. Wireless sensor node resources are restricted, particularly regarding of computing and energy. Those nodes are frequently used in unattended and complex situations. WSNs are subject to node capture, Sybil threat, and black-hole attacks, among others. More academics are looking at how to increase network performance by efficiently defending against rogue nodes [3]. Trust-based systems have been shown to highly resistant to internal node threats in WSN security. A trust-based technique is useful for forecasting node behavior in the future based on previous observations and finding an appropriate decision depending on suspicious node behavior; this gives a novel solution for WSN routing security. Traditional trust aware routing protocols, on the other hand, have several limitations, such as high energy consumption and a limited number of forms of defendable attacks [4]. WSNs are very vulnerable to attacks because to their open and dispersed nature and the limited resources of the sensor nodes. Furthermore, packet broadcasting is required often in WSNs, and sensor nodes can be installed at random in an environment, allowing an attacking opponent to quickly infiltrate a WSN [5].

Sensor nodes are tiny, mobile devices that can communicate, perceive, and analyse data in a larger network. These have a restricted transmission range and therefore send data straight to the intended recipient. Because WSNs are prone to internal and external outbreaks, data transmission over greater distances can be done through intermediary nodes. Most of the time, due to their limited resources, they are unable to deal with a strong opponent. In this circumstance, a secondary defensive system, also known as an intrusion detection system, is necessary. With aid of an intrusion detection system, the attacker activities can be identified. The confidence and faith that a node has in the competency, consistency, and trustworthiness of other nodes is known as Trust8. Firsthand trust, often known as first-hand information, is based on direct observation of a node [6] [7].

As a second wall, an intrusion detection system plays a critical role in safeguarding the WSN by detecting node misbehavior that breaches the security procedures. Complex security mechanisms are challenging to use in a WSN because they enhance the SN energy consumption. As a result, WSNs use light-weight security measures to safeguard the network, and IDS provides a platform by recording SN misbehavior and reporting it to the administrator for countermeasures. An attacker can use packet dropping and alteration to interrupt communication in wireless multihop sensor networks. Several strategies to reduce and lessen such attacks have been presented, but only a handful can properly and efficiently detect the invaders. Multipath forwarding is a frequently utilized countermeasure for packet drops [8] [9].

We have primarily concentrated on the anomaly detection system in this research. The authors proposed a trust-based system as an IDS for WSN. In this paradigm, every SN trust is determined individually at the physical layer, MAC layer, and network layer using trust metrics. Ultimately, the trust values of every layer are added together to generate a single overall trust value.

The following security requirements and difficulties should be addressed in a secure data connection.

- In order to avoid intruders, sensor nodes should communicate with all other nodes.
- At the moment of transmission, data packets transferred over a network must not be manipulated by any adversary.

- All sensor nodes must communicate securely, and data must be safeguarded.
- The identities of all sensor nodes must be validated.
- A substantial quantity of data will be lost if the intruder nodes are not detected and removed from the network soon.
- Even if the multiple routing network is able to identify itself only from a few kinds of networks attacks, it is still exposed to serious security concerns.
- The main purpose of the WSN is to save energy, which extends the network lifetime and reduces data loss.

2. LITERATURE SURVEY

Rizwana et al. [1] proposed an anti-packet-dropping intrusion detection system algorithm. The problem is solved by an intrusion detection algorithm that analyses the network and detects abnormal nodes. The abnormal node is then converted to a normal node using an intrusion detection method. This proposed IDS is employed to detect and separate hostile nodes from network, and proposed methodology reduces packet loss and improves network performance when compared to the existing algorithm.

Although TESRP is among one greatest trust-based safe routing protocols available, it does not protect against wormhole attacks. This work uses a trust-based method and the sequencing notion to guarantee security against wormhole attacks in TESRP. With respect to residual energy, throughput, PDR, E2E delay, simulation results indicate a comparison of TESRP values in three areas [3].

To identify and isolate rogue nodes, the authors in [4] present an Energy-optimized Secure Routing (EOSR) formed on distributed trust evaluation model. EOSR routing protocol devised a multi-factor routing approach that took into consideration trust level of node, the remaining energy, and the path length. This method not only means that the data is routed via trusted nodes, and it also ensures that energy consumption is distributed evenly across them.

In this study, Huangshui Hu et al. [5] offer a TSRP for WSNs to guard against various attacks. Every node assesses the complete trust values of its neighbours based on direct trust value, indirect trust value, volatilization factor, and residual energy to combat black hole, selective forwarding, wormhole, hello flood, and sinkhole threats. Then, every source node that wants to transfer data to its neighbours sends a multi-path routing request packet to its neighbours, and the process continues till the sink at the end is achieved. Finally, depending on the path entire trust values, transmission distance, and hop count, the sink analyses the incoming packets to find the optimum path. As per simulation results, TSRP has lower network latency, packet loss rate, and average network energy consumption than ad hoc on-demand distance vector routing and trust based safe routing protocol.

An ANN is trained on database to identify and categorise distinct DoS attacks, according to Iman Almomani et al. [6]. WSNDS increased IDS' capacity to attain greater classification accuracy rates, according to the findings. The holdout and 10-fold cross validation procedures were utilized with the WEKA toolkit. With 10-fold cross validation and one hidden layer, the best results were obtained. In addition to the typical scenario (without attacks), the classification accuracies of Blackhole, Flooding, Scheduling, and Grayhole attacks were 92.8%, 99.4%, 92.2%, 75.6%, and 99.8%, correspondingly.

The Advanced Sybil Attack Detection approach is being established, while Wormhole Resistant Hybrid Technique is being used to detect wormhole attacks. Rupinder Singh et al. [7]. The signal intensity and distance are used to identify hello flood attacks. An experimental study is performed on a collection of nodes; 13.33% of the nodes are identified as misbehaving nodes that classified attackers and provided a true positive rate and false positive rate detection rate. The Sybil attack is discovered at a rate of 99.40%, while the hello flood attack is detected at 98.20% and the wormhole attack is detected at 99.20%.

IDS was presented by Syed Muhammad Sajjada et al. [8], in which each node monitors the trust level of its neighbours. Neighboring nodes might be classified as trustworthy, dangerous, or malevolent based on their trust values. For packet forwarding reasons, the forwarding engine recommends trustworthy nodes. By evaluating network statistics and malicious node activity, the proposed technique successfully identifies Hello flood attack, jamming attack, and selective forwarding attack. Simulation findings suggest that when a neighbour node trust management-based anomaly detection approach is used, the network operates better.

The WSN is secured by Umashankar Ghugar et al. [9] LB-IDS which detects jamming attacks, back-off manipulation attacks, sinkhole attacks, and cross-layer attacks at the physical, MAC, and network layers, correspondingly. Every tier trust threshold parameters are being used to differentiate among malicious and legitimate nodes in the network. With respect to message complexity, memory overhead, energy usage, and trust evaluation, LB-IDS is likewise subjected to a -e research. LB-IDS will be a better security choice for clustered WSNs.

3. SECURE DATA COMMUNICATION MODEL

3.1 INTRUSION DETECTION SYSTEM

An IDS detects intrusions that attempt to access a resource integrity, confidentiality, or availability. Data collection, detection, and reaction are the three basic components of IDS. Data collection and pre-processing tasks like data translation to a common format, data storage, and data transfer to the detecting module are handled by the data collecting element. IDS can take input from system logs, network packets, as well as other data sources. The detection element processes data to determine intrusions, while the response element receives indicators of intrusions.

If the attacks cannot be prevented or detected effectively, WSNs will not be able to perform well in the mission critical area. Some security techniques, like malicious node detection and acknowledgement, were brought to the region to mitigate the consequences of such selfish or malicious nodes WSNs. All the security systems, however, suffer from a late finding fault, that gives attackers plenty of opportunity to disrupt network performance. Moreover, because of the unique characteristics of WSN infrastructure, such as open medium, rapid topology changes, and a lack of centralised monitoring, prevention techniques alone are no longer sufficient to protect WSN from outside attackers; and hence, an IDS must be added to improve its security. If IDS can identify intruders as soon as they access the network, it will be able to entirely prevent them from causing any network harm. In WSNs, IDS might serve as a second line of defense.

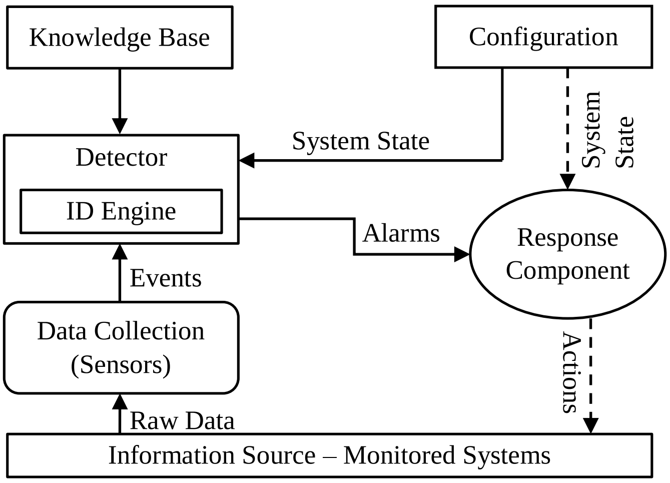

Fig.1. IDS and data collection

Second layer of a security system is commonly referred to as the intrusion detection system. Intrusion Detection (ID) can be carried out in two ways: attacks from outside the computer environment or network, and Misuse from within the network. Intrusion detection can be classified with neither host-based nor network-based based on audit data. A network-based IDS collects and analyses network traffic packets, whereas a host-based IDS looks via operating system or application logs. Based on detection approaches, IDS may be split into three categories: anomaly-based intrusion detection, misuse-based intrusion detection, and specification-based intrusion detection. Nodes might be classified as dysfunctional, selfish, or malignant based on their behavior. Hardware problems or software faults cause malfunctioning nodes. Data packets are not forwarded or discarded by selfish nodes. It can participate in the route discovery and maintenance stages, and it will not forward data packets to save resources. Malicious nodes employ their resources to bring down other nodes or the whole network by seeking to engage in all known routes and forcing another nodes to use a destructive route they control.

3.2 INTRUSION PREVENTION SYSTEMS (IPS)

Secure data transfer is intended to keep data safe from illegal access, damage, or disruption. In this proposed work, an intrusion prevention system is being meant to tackle the continuously growing threats offered by the current generation of malware, software, and exploits. As the number of intruders has grown, the network environment has become more complicated, making threat mitigation more difficult. Modern wireless sensor networks have emerged for the aim of transmitting important information and services to an ever-growing set of users. Because of the necessity for access to these important services, redundant communication lines, wireless networks, mobile notebook computers, portable digital devices, and even internet-enabled cellular phones have all been developed. These new access methods and linkages boost the value of the information systems they support, but they also open up more attack and compromise points. This paper will discuss the necessity for Intrusion Prevention Systems, examine the two most common IPS architectures, and attempt to give guidance on how to choose and operate these systems.

Intrusion Detection Systems (IDS) were created to detect and notify threats to security staff for manual repair. Traditional intrusion detection solutions do not prevent attacks; instead, they identify hostile traffic and give notifications. The amount of time required to assess and respond to IDS systems became excessively huge as the degree of threats and the extent of IDS installations expanded.

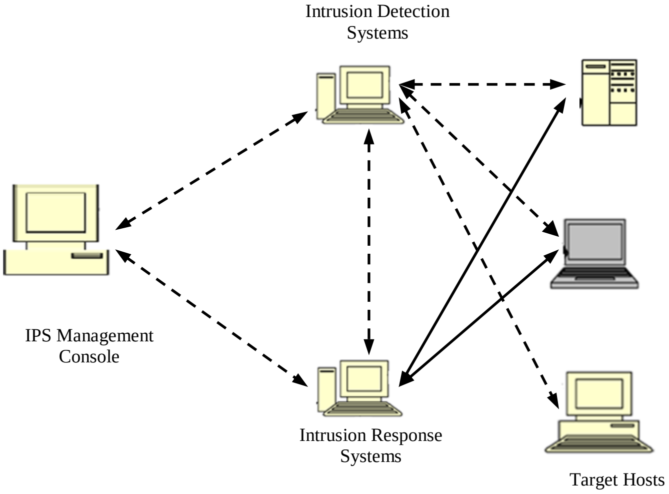

Fig.2. Intrusion Prevention System

The emergence of new hybrid threats that compromise security infrastructure via many avenues has underlined the necessity for businesses to defend themselves against a continuously changing threat. As breaches have gotten more aggressive, organizations have experienced catastrophic harm to their business confidentiality, integrity, and availability.

Function of Intrusion prevent ion System

- Identifying harmful node activity
- Logging information about it
- Attempting to prevent or halt it
- Reporting the activity

Currently, there are two fundamental techniques to attaining the above-mentioned objectives.

- **Host Intrusion Prevention**: A software system that is installed directly on the computer system that is being safeguarded.
- **Network Intrusion Prevention**: A specialized software or hardware solution that links to a network segment and protects all systems connected to the same or downstream network segments.

3.3 NETWORK INTRUSION PREVENTION SYSTEM

Network IPS devices are placed in front of the network segment that needs to be secured. The Network IPS device must process all data flowing among protected segment and remaining network. Traffic is evaluated for the presence of an attack as it goes through the device. The most accurate systems use numerous strategies to obtain very high levels of confidence in the detection of threats and misuse.

Because misidentification of an attack might result in valid traffic being stopped, a self-inflicted Denial of Service scenario, extreme precision and high levels of performance are critical to an effective system. To guarantee that valid traffic is not delayed or disturbed as it passes through the device, high performance is required. While an attack is detected, Network IPS rejects or prevents criminal data from reaching the proposed target, effectively stopping the threat.

4. SECURITY REQUIREMENTS

Attack prevention, detection, and resilience are all aspects of computer security. Because sensor networks are frequently deployed in unsupervised environments, it is usual to focus on attack survivability, or the capacity to withstand an attack while continuing to function normally. Depending on the application, a secure protocol may be required to have a number of qualities. The most important security criteria are outlined here.

- ***Confidentiality or Privacy***: The protection of unlawful access to information is characterized as confidentiality or privacy. Information is disclosed as a result of a breach of confidentiality.
- ***Integrity:*** is described as the prevention of illegal change or destruction of data, whether unintentional or malicious. By changing or deleting data, we are manipulating the authorized entity and giving him incorrect information.
- ***Authentication:*** The act of confirming an entity claimed identification is known as entity authentication, whereas data origin authentication is known as the process of verifying the data source, which implies data integrity.
- ***Availability:*** The percentage of time a system is operating and available to the user is referred to as availability. It describes the capacity to gather data from sensors in the context of a sensor network. Although it is not a direct security need, we consider it to be part of the security requirements since an adversary can use various threats to interrupt the sensor network regular operation.
- ***Data freshness:*** An attacker should not be able to reuse previously authenticated communications.

5. PROPOSED METHOD

Incorporating group based trust management systems in a wireless sensor network to dynamically choose the cluster head depending on the energy profile of every node and to perform safe routing.

5.1 MULTI HOP TRUST MANAGEMENT SCHEME

Two topologies are used in the proposed trust model. The intragroup topology, for example, employs distributed trust management. Intergroup topology, on the other hand, adopts a centralised trust management technique. For intra group network, each sensor in the group determines individualized trust values across all group members.

Depending on the trust values, a node assigns one of three possible states. To other member nodes, they are 1) trustworthy, 2) untrusted, and 3) uncertain. The three-state approach was selected because of its mathematical simplicity and ability to handle the problem in enough depth. Every node then sends the trust state among all group member nodes to CH. Then there centralised trust management to consider. Depending on the trust statuses among all group members, a CH identifies the malicious node(s) and transmits a notification to the BS. Every CH also sends the BS the trust values of other CHs upon request. Whenever this information reaches the BS, it assigns one of three possible states to the whole group. The BS will inform the CHs of the present situation of a certain group upon request. The three phases of our group-based trust model are as follows:

- Calculation of trust at node level
- Calculation of trust at cluster-head level
- Calculation of trust at BS level.

The Fig.3 shows the multi hop trust management based secure data transmission.

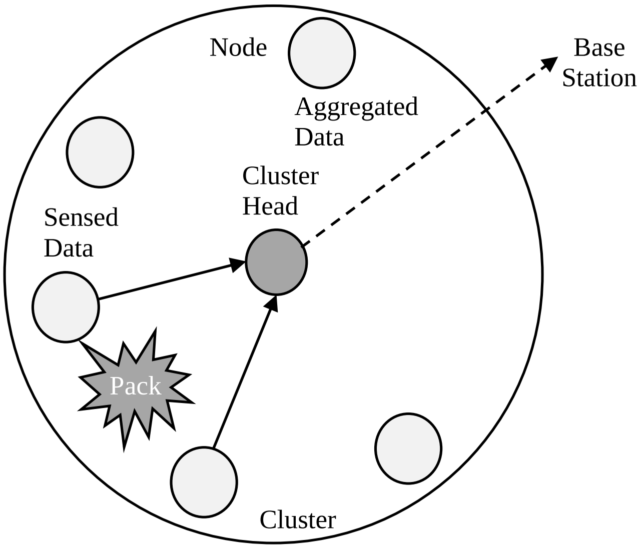

Fig.3. Multi Hop Trust Management based secure data transmission

The trust value is calculated by MHTM using direct or indirect observations. Indirect observations reflect the suggestions of trustworthy peers regarding a certain node, whereas direct observations indicate total successful and failed interactions. The term interaction refers to two nodes working together. If a sender receives confirmation that the packet was successfully received by the neighbor node and that the node transmitted the packet to its destination in an unmodified state, the interaction is considered successful.

As a result, the first criteria, successful reception, is met when the link layer acknowledgement is received (ACK). IEEE 802.11 is a standard link layer protocol that caches messages until the sender gets an acknowledgement. The sender receives an ACK whenever the receiving node gets the message appropriately. The sender node will restart the packet if it does not get the ACK within a particular length of time.

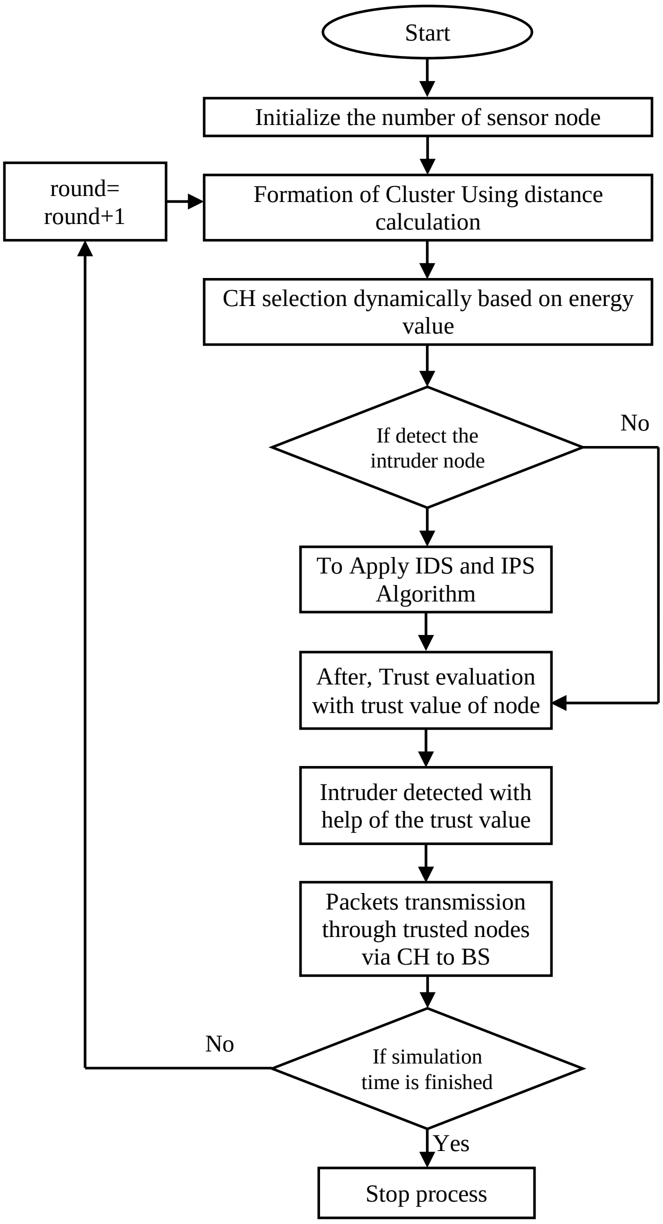
Start
Initialize the number of sensor node
round= round+1
Formation of Cluster Using distance calculation
CH selection dynamically based on energy value
If detect the intruder node
No
To Apply IDS and IPS Algorithm
After, Trust evaluation with trust value of node
Intruder detected with help of the trust value
Packets transmission through trusted nodes via CH to BS
No
If simulation time is finished
Yes
Stop process

Fig.4. Intra Group to Base Station

Algorithm for Detection

```
Start:
Initialize the number of sensor node
Step 1: Select Maximum Energy Node as CH
Step 2: CH node broadcast RREQ packet.
Step 3: NCH receives RREP, RIE of ICH.
Step 4: Received timestamp of RREP by NCH< MN Make current NCH as Malicious node
Step 5: If malicious Node are identified
        a. delete RIE of NCH from Source Routing Table
        b. Send malicious node id to BS
Step 6: Else
        a. MNI will free its buffer Packets dropout by MNI so read other packets
        b. BS after received id of intruder by MNI node
        c. Update buffer for given time limit in every round
        d. Packets arrival rate should be less than destination
Step 7: if TH value > routing path;
        a. Current TH> neighbor TH
Step 8: Then, suspect node=$i$
        a. Suspect node = current TH
        b. count=count + $r$
Step 9: End if
```

Algorithm for Prevention

```
Step 10: After, finding the malicious node to check false reply route using AOMDV
Step 11: Sender node starts route discovery to locate receiver node
Step 12: Update the minimum node count of the route in destination
Step 13: If sender detects the false reply route
         a. Then, sender sends more RREQ
Step 14: Else
         a. There is no detect the false reply route
         b. Data sends through the BS
Step 15: Repeat the process while the time is finished.
Step 16: while (current time ≤ (current time + wait time))
         {
         Store the RREP destination id and source id in RR table
         }
Step 17: if (destination id> source id)
         {
         Malicious id= source node id
         Discard entry from the table
         }
Step 18: Stop
```

The second criterion, packet forwarding, is satisfied by adopting enhanced passive acknowledgment (PACK) by overhearing the broadcast of a next hop on the path since they are within radio range. If the sender node does not hear the neighbouring node retransmission of the packet within a certain amount of time, or if the overheard packet is discovered to be illegally fabricated (by comparing the payload attached to the packet), the sender node will consider the interaction to be unsuccessful. If the number of unsuccessful interactions increases, the sender node trust value drops, then the adjacent node may be perceived as broken or malicious.

5.2 TRUST CALCULATION AT CLUSTER-HEAD

In this case, the study will suppose that the CH is the SN with the most processing power and memory among the SNs.

5.2.1 Trust State Calculation of Intra Group:

CH requests nodes for the trust statuses of other members in the group to determine the global trust value of nodes in a group. For two reasons, we employ trust states rather than actual trust values. First, because just a basic state has to be conveyed to the

CH, the communication overhead would be reduced. Secondly, a particular node trust boundaries differ from those of other nodes.

For one node, a given trust value may belong to the trusted zone, while for another node, it might relate to unsure zone. As a result, calculating the global trust state of nodes in a group using only trust states might be more possible and efficient. Let say the group has *n* nodes, including CH. CH transmit request packet to rest of the group on a regular basis.

As a result, complete member nodes send the CH their trust statuses, s, of other group member nodes. Variable *s* can be in one of three states: trusted, uncertain, or untrusted. CH will keep track of various trust states in the form of a matrix, as illustrated below

(1)

where T_{Mch} indicates trust state matrix of cluster head *ch*, and *sch*, 1 indicates state of node 1 at cluster head *ch*. Depending on the specific difference in trust states for that node, the CH gives a global trust state to that node. A basic normal distribution is used to simulate this relative difference. As a result, the CH will create a random variable *X* in such a way that

(2)

The study describe total of *m* such random variables as S_m, supposing this is a uniform random variable. Because of the central limit theorem, Sm will behave like a regular variable. This random variable has an expected value of m and a standard deviation of $\sqrt{m}/3$. For a node *j*, the CH specifies the following standard normal random variable,

(3)

When $Z_j \in [-1, 1]$, then node j is called as uncertain, otherwise if $Z_j>1$, it is termed to be trusted. When $Z_j<-1$, it is untrusted.

6. RESULT AND DISCUSSION

The WSN with 50 nodes is formed in NS-2.34 version and the parameters are presented in Table.1.

Table.1. Simulation Parameters

Parameters	Values
Number of Node	50
Area Dimension	800×800 m
Routing Protocol	AOMDV
Total Energy	150J
Initial value of Energy	1.5J
Maximum Packet Size	4000 bits
Simulation Time	60s
Type of the MAC	802.11

An energy model is used to calculate the energy of each node. Now the energy calculated for the nodes is compared with one another and the node with higher energy is found. This node with higher node energy is assumed as the cluster head. As a next step the trust values of 50 nodes are computed considering successful and unsuccessful transmissions. If trust value of the node is 2 then the node is trusted node. When trust value is other than 2, then nodes are considered untrusted according to the Group based trust management scheme. Now trusted nodes are found and their node color is changed. After finding the trusted nodes the transmission between the trusted nodes occurs and finally the packets are transmitted to the cluster head.

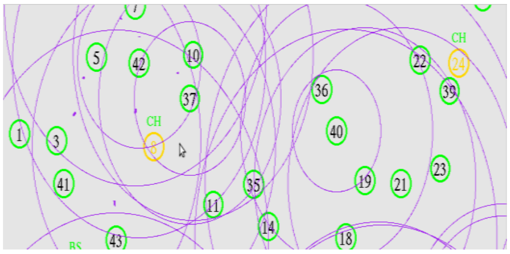

Fig.5(a). Packet transmission

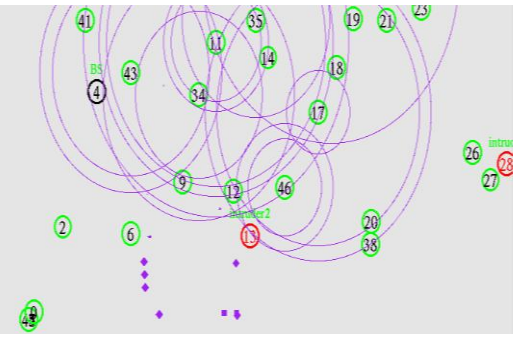

Fig.5(b). Packet drop

Now the trusted nodes are found and their node color is changed. After finding the trusted nodes the transmission between the trusted nodes occurs and finally the packets are transmitted to the cluster head. If there is any transmission between untrusted then there is some packet drop. Finally draw chart for the required parameters. The Fig.5 mentioned that fewer than red color nodes are intruder nodes (or) untrusted node, so that the intruder nodes are dropped all the packets.

The Proposed Methodology MHTM is meant to prevent this by adding the authentication method and transferring the trust values. Traffic is monitored by establishing timestamps after the link between nodes is created. The trust value is a random key that is supplied with each request. The proposed MHTM approach is compared to the current TSRP trust aware technique.

6.1 PACKET DELIVERY RATIO

First validation is regarding packet delivery ratio measurement among TSRP and proposed MHTM techniques.

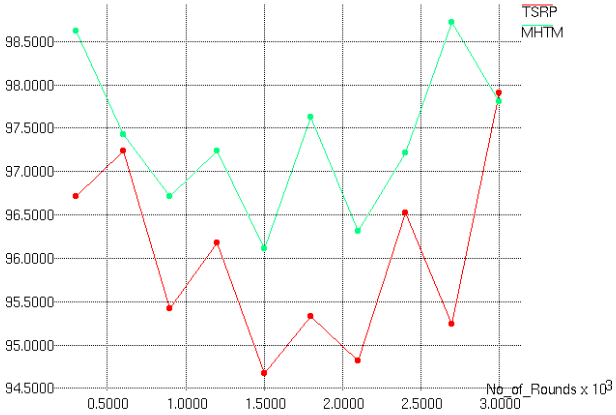

Fig.6. Packet delivery ratio

For both existing and proposed techniques, packet delivery is increased. For MHTM technique, the trust value of every node is an extra process that has to be followed by the network. This indicates MHTM technique performs well with making increased of PDR.

6.2 ENERGY CONSUMPTION

The second parameter to validate proposed technique is energy consumption. The energy consumption is the energy loss taken to transmissions of Packets. In the proposed MHTM technique, the energy consumption is found to be reduced as depicted in below Fig.7.

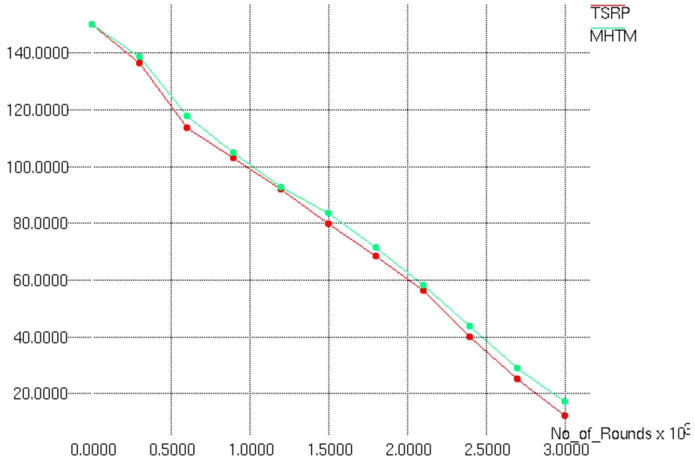

Fig.7. Energy consumption

From the Fig.7, energy consumption for the proposed method MHTM is reduced in contrast with existing TSRP method. Energy Consumption is reduced 3%. As a result of the lower energy use, authentic users will experience speedier traffic. In this study, both current and proposed strategies are put to the test on a network arrangement.

6.3 END TO END DELAY TIME

The average time it takes for a data packet to arrive at its destination is known as the packet delivery delay. It also includes the time lost as a result of the routing procedure. Only data packets that are transmitted to their intended destinations are counted.

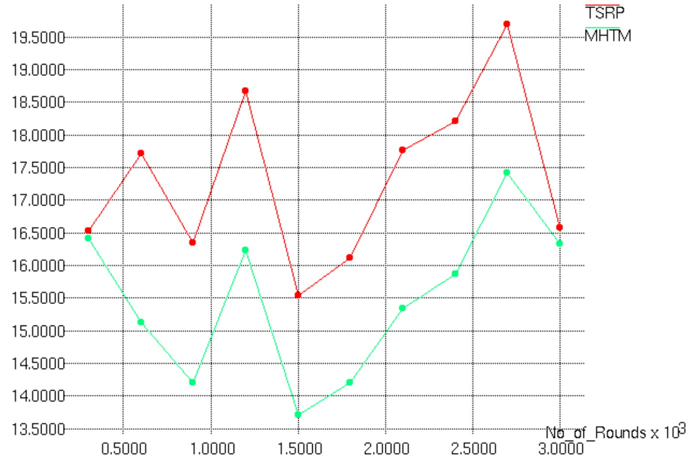

Fig.8. Delay

The Fig.8 shows Packet delay time with respect to transmission time. This shows that TSRP technique performs well with decrease in packet delivery delay time. The data transmission average delay of TSRP is 19.128ms and MHTM is 16.43ms. From Fig.8, it is found that MHTM has better performance.

7. CONCLUSION

Security is most important issues in wireless sensor network. Using our propose approach Multi Hop Trust Management (MHTM) technique is used to identify the trusted nodes with malicious node directions for efficient and secure communication in any kind networks. Intrusion Prevention System (IPS) is the only proven defense against today complex attacks in network settings. In this proposed work is provides high transmission of packet delivery ratio to enhance network lifetime efficiency regarding time, and at the same time, packet losses while intruder nodes. The MHTM technique uses for detecting malevolent nodes and avoided number of packet losses in the WSN.

REFERENCES

[1] S. Rizwana, K.M. Gayathri and N. Thangadurai, “Intrusion Detection Algorithm for Packet Loss Minimization in Wireless Sensor Networks”, *International Journal of Engineering and Advanced Technology*, Vol. 8, No. 6, pp. 69-74, 2019.

[2] T. Karthikeyan and K. Praghash, “Improved Authentication in Secured Multicast Wireless Sensor Network (MWSN) using Opposition Frog Leaping Algorithm to Resist Man-in-Middle Attack”, *Wireless Personal Communications*, Vol. 113, pp. 1-17, 2021.

[3] T. Karthikeyan and K. Praghash, “Data Privacy Preservation and Trade-off Balance Between Privacy and Utility Using Deep Adaptive Clustering and Elliptic Curve Digital Signature Algorithm”, *Wireless Personal Communications*, Vol. 116, pp. 1-16, 2021.

[4] R. Manikandan and M. Ramkumar, “Design of Autonomous Production using Deep Neural Network for Complex Job”, *Materials Today: Proceedings*, Vol. 4, pp. 1-12, 2021.

[5] Huangshui Hu, Youjia Han, Hongzhi Wang, Meiqin Yao and Chuhang Wang “Trust-Aware Secure Routing Protocol for Wireless Sensor Networks”, *ETRI Journals*, Vol. 20, No. 1, pp. 674-683, 2021.

[6] Iman Almomani, Bassam Al-Kasasbeh and Mousa AL-Akhras, “WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks”, *Journal of Sensors*, Vol. 2016, pp. 1-16, 2016.

[7] Rupinder Singh, Jatinder Singh and Ravinder Singh “Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks”, *Wireless Communications and Mobile Computing*, Vol. 2017, pp. 1-15, 2017.

[8] Syed Muhammad Sajjada, Safdar Hussain Boukb and Muhammad Yousafa, “Neighbor Node Trust Based Intrusion Detection System for WSN”, *Proceedings of International Conference on Emerging Ubiquitous Systems and Pervasive Networks*, pp. 183-188, 2015.

[9] Umashankar Ghugar, Jayaram Pradhan, Sourav Kumar Bhoi and Rashmi Ranjan Sahoo, “LB-IDS: Securing Wireless

Sensor Network using Protocol Layer Trust-Based Intrusion Detection System", *Journal of Computer Networks and Communications*, Vol. 2019, pp. 1-14, 2019.

[10] Gonugunta Tulasi and R. Suresh, "Secure Data Transmission in Wireless Sensor Networks: Against Packet Dropping Attacks", *International Research Journal of Engineering and Technology*, Vol.3, No. 7, pp. 2386-2389, 2016.

[11] Sushant Kumar Pandey "An Anomaly Detection Technique-Based Intrusion Detection System for Wireless Sensor Network", *International Journal on Wireless and Mobile Computing*, Vol. 1, No. 4, pp. 323-333, 2019.

[12] Zhang Huanan, Xing Suping and Wang Jiannan, "Security and Application of Wireless Sensor Network", *Proceedings of International Conference of Information and Communication Technology*, pp. 486-492, 2021.

[13] Xinying Yu, Fengyin Li, Tao Li, Nan Wu, Hua Wang and Huiyu Zhou, "Trust‑Based Secure Directed Diffusion Routing protocol in WSN", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 43, pp. 1-13, 2020.

[14] Hanane Kalkha, Hassan Satori and Khalid Satori, "Preventing Black Hole Attack in Wireless Sensor Network using HMM", *Proceedings of International Conference of Intelligent Computing in Data Sciences*, pp. 1-12, 2018.

[15] Parmar Amisha and V.B. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol", *Proceedings of International Conference on Communication, Computing and Virtualization*, pp. 1-8, 2016.

[16] Reem Alattas, "Detecting Black-Hole Attacks in WSNs using Multiple Base Stations and Check Agents", *Proceedings of International Conference on Future Technologies*, pp. 1020-1024, 2016.

[17] Mohammad Wazid, Avita Katal, Roshan Singh Sachan, R.H. Goudar and D.P. Singh "Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network", *Proceedings of International conference on Communication and Signal Processing*, pp. 576-581, 2013.

[18] Jitendra Kurmi, Ram Singar Verma and Sarita Soni, "An Efficient and Reliable Methodology for Wormhole Attack Detection in Wireless Sensor Network", *Advances in Computational Sciences and Technology*, Vol. 10, No. 5, pp. 1129-1138, 2017.