International Journal of Engineering & Technology, 7 (4) (2018) 2746-2751

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.17957
Research paper

Improve secure based multi-path routing to mitigate the intrusion endurance in heterogeneous wireless sensor networks

Dr. G. Murugan*

Professor, Dept. of Computer Engineering, Vidyalankar Institute of Technology, Wadala (East), Mumbai
**Corresponding author E-mail:gopalmurugan0@gmail.com*

Abstract

Wireless Sensor Networks (WSNs) have many potential applications. Multi-path routing is widely used in WSN to achieve reliability and perform Fault Tolerance. Multi-path routing determines and assigns multiple routes from a given sensor node to the sink. The transmission of data among the multi-path brings path redundancy, which increases the reliability and reduces the network congestion. In this research work, a dynamic redundancy management algorithm is proposed. To exploit multi-path routing in order to process the user request with existence of defective and malicious nodes. The objective of this work is to analyze the trade-off between energy consumption and Quality of Service (QoS) gain in security and reliability in order to increase the lifetime. The optimized redundancy level of multi-path routing is determined dynamically which is used to improve the query response while extending the network lifetime and also for detecting intrusions and send alert to the system through Intrusion Detection System (IDS). Then, a voting-based distributed Intrusion Detection (ID) algorithm is proposed to detect and remove malicious nodes in a sensor network. The malicious node has been determined through number of voters using voting-based distributed ID algorithm. The efficient redundancy management of a clustered Heterogeneous Wireless Sensor Network (HWSN) is to increase the network lifetime in the presence of unreliable and malicious nodes. Therefore, the reliability improved dramatically.

Keywords: *Multipath Routing; Energy Conservation; Heterogeneous Wireless Sensor Networks; Intrusion Detection; Security.*

1. Introduction

Wireless Sensor networks (WSNs) is a network that consist of small, lightweight sensor nodes, distributed in random manner. Sensor Nodes (SN) are deployed in large numbers to supervise the system by the measurement of physical parameters such as temperature, pressure, or relative humidity. WSN is an important research area in networks. And its application includes general engineering, environment science, health service, military, etc. The essential operations performed by WSNs are data dissemination and data gathering. SN is a small device with restricted memory, energy and transmission range. WSNs are densely deployed and topology of sensor network changes frequently. In general, the vital goal of a WSN is to guarantee the observation of a given area with a restricted number of sensors and finally transmit the sensed data to the processing unit. As a result, in WSNs there is need for efficient reliability and less delays during communication. In general: a computing subsystem; a communication subsystem short a sensing subsystem; and a power supply subsystem constitute the wireless sensor network.

The QoS demands like reliability, timeliness and security are not met in sensor network due to their limited resource availability. Moreover, there is also reduced energy consumption for extending the system lifetime. Exchange amid Reliability and energy consumption reported earlier excluded the transfer of malicious node in the network along with packets. Intrusion Detection System (IDS) is used to identity and arrests such malicious nodes. This process leads to rapid consumption of energy which is not reported in previous studies. There are also chances of path break due to inside attackers. This usually happens in Heterogeneous sensor network. Here, the cluster head actively collects and forwards sensed data to sink node and they are also helpful in augmenting the network performance.

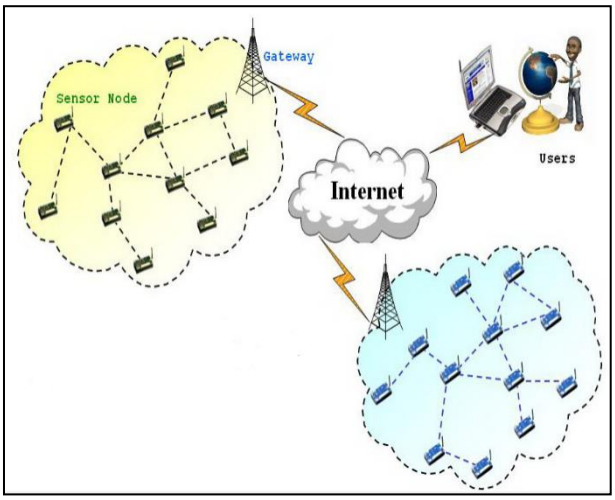

Fig. 1: Wireless Sensor Network Architecture.

Figure 1. Represents the architecture of sensor network in which the sensor nodes send the required data to the sink node. In general the sensor network is energy limited and leads to some attacks due to its open nature. The main design consideration of security protocols is dependent on symmetric keys. But the symmetric keys are exchanged for every transformation of data. Therefore, this type of keys results in overhead and complex computation.

1.1. Routing in WSNS

In WSNs, transmitting data from target area to the sink node is an important task and the technique employed to transfer data packets from one sink node pair to another is a significant subject to be considered while developing these networks. Routing is an important issue in low-power WSNs [1], [2].Generally, sensor nodes are distributed in random manner, and routing protocols can maintain the data transmissions over an extended distance apart from the network size. Energy depletion may affect the network operation, so that after performing the task, the node can be moved to sleep node. The routing can be classified as, hierarchical-based routing, flat-based routing and location-based routing. A sink node requests the stream of data from sensor node. The node which sends the request data is referred as source node.

1.2. Multipath routing

Multi-path routing apart from being an efficient technique for Fault and Intrusion Tolerance also considerably enhances the data delivery. The trade-off between energy consumption and reliability, security exists while the data sent from source to sink shortens the lifetime of the network [13]. The main task of routing is making data structures which have information on how a given sink can be reached. Routing involves two types of protocols: Proactive: The protocol is active before that table is needed and Reactive: Route is only determined when actually needed. In single path routing, there is a single path between source node and sink node. This routing provides simple data forwarding through the nodes. Any failure occurs over the path, there is loss of data and delay.

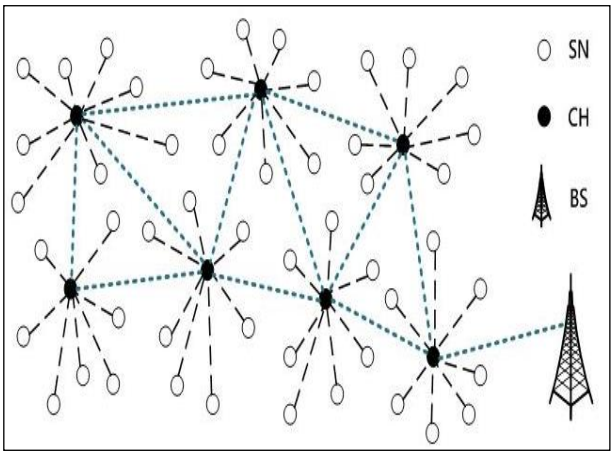

Fig. 2: Multi-Path Routing in Wireless Sensor Network.

Figure 2. Describes the mutli-path routing in sensor network. Multi-paths are available to send the data, so the data reach the destination without any changes. The probability to reach the sink has high reliability. In that diagram, the sensor node sends its data to their Cluster Head (CH) and the CH forwards the data to the appropriate base station. The same data is sent through multi-path routing, path redundancy and source redundancy occurs. The number of paths trusted to send the same data to sink is called path redundancy. Source redundancy is to trust the source nodes in the network to send the sensed data.

1.3. Intrusion tolerance through multi-path routing

The main issues in multi-path routing are the number of paths to be used and optimal path to be selected for secure transmission. To avoid the problem the trusted nodes allow sending the data in the network. The trusted nodes are found by voting based IDS which done locally to save the energy.

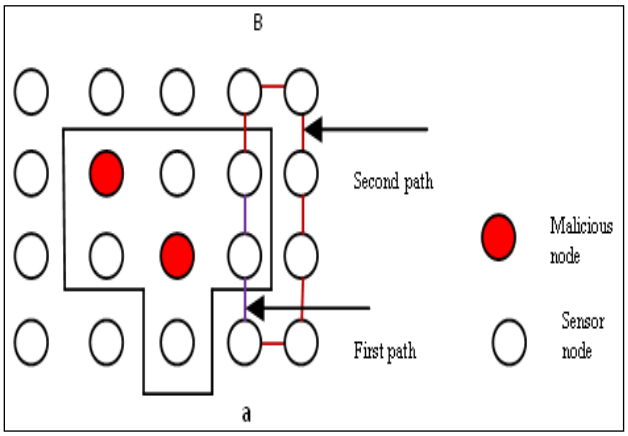

Fig. 3: Tolerates the Intrusion Through Muli-Tple Routes.

Figure 3. Represents the multiple routes existing from source to sink. When a message is sent from source to destination, more than one path is available in order to tolerate the intrusions. The red color node is represented as a malicious node and it affects the neighbor node also. The path from node A to B is considered as the shortest path, but due to malicious node it infects the neighbor node also. For this reason, the second path is chosen, in which there is a possibility to reach the sink in reliable manner. Within the box, the nodes are considered as infected nodes. These malicious nodes are detected through voting based algorithm [3]. Here, to save the energy Voting-based Intrusion Detection System is used.

The remaining sections are as follows. In Section II, the related works are described where the proposed approach is differentiated with prior work. In Section III, the proposed methods and methodologies are explained for tolerating the intrusions in order to increase the reliability. In Section IV, Mathematical model is evaluated for analyzing the energy consumption. In Section V, numerical data is provided and performance is evaluated. In Section VI, the paper is concluded and some future research work is pointed.

The summery of this work is to analyze the trade-off between energy consumption and QoS gain in security/ reliability in order to increase the lifetime. A dynamic redundancy management algorithm is proposed to improve the network lifetime. The role of the Proposed Voting-based Distributed ID algorithm is to detect and remove malicious nodes in a WSNS. The malicious node has been determined through number of voters using Voting-based Distributed ID algorithm. The efficient redundancy management of a Clustered HWSN is to increase the network lifetime in the presence of unreliable and malicious nodes. The reliability improved dramatically.

2. Related works

Kang et al 2006 described about the routing insecure manner. In geographic routing, the established path is done through by analyzing location information. In a potential attack, malicious nodes may falsify their location information. Also, this routing sends excessive number of packets to overload the receiving nodes. In addition, there is drop/misdirection of received packets. To remove these problems, the author suggests secure geographic protocol which considers the parameters such as, packet scheduling,

rate control and trust-based multi-path routing. By using them, they achieve a considerable higher delivery ratio with low congestion. This technique dynamically avoided untrusted paths and continues to route packets even in the presence of attacks.

Felemban et al (2007) described about the attacks occurred in sensor network and detection of attacks by IDS. Felemban et al (2006) proposed MMSPEED protocol to achieve high reliability. But the proposed protocol requires complex computation for selecting the path for data transmission.

Cheng et al (2007) analyze the performance of admission control algorithm. New request may get rejected if no available resource was left. Failure of accepting a high-priority request would incur high penalty to the system. Dynamic-threshold based admission control algorithms accept all requests and provide QoS. Dynamically adjusting resources are essential to achieve high system performance (38%). The author planned the algorithm based on the characteristics of the system workload. This algorithm lowers service requirements of low-priority requests in order to reduce the loss. Overhead occurred due to the need of common pool to share. And it requires expensive complex computation. The author did not consider about the overflow of pool which caused congestion during requesting the service.

Based on the observations of node, intrusions present in the Network are detected. In IDS, the Monitor Node easily gets compromised and is also vulnerable to threats. Carol (2011) suggested the collaborative technique for Intrusion Detection System (IDS). This problem is avoided and Collaborative Intrusion Detection Network (CIDN) improves the detection. CIDN detects the intrusion based on knowledge, experience and collective information shared among peer. And it has the ability to detect the intrusions in accurate manner. In Centralized Collaboration system, the system gets failed when bottleneck occurs in sensor network. To protect the CIDN from Malicious Nodes, trust is needed to evaluate the performance of each node. Here, Dirichlet Trust Management Model is used and acquaintance Management Algorithm is also proposed to enable accurate intrusion detection. This also reduces the overhead dramatically. In CIDN, a trust model is proposed to calculate the trustworthiness of Host-based Intrusion Detection System. This is scalable and robust to the common threats occurring in the network. Compared to previous work, this work is more effective involving detection of the intrusions and providing security a required for communication performed between the networks.

The data transfer in WSN is described by Fenyeet al (2012). In previous papers they concentrated only on common attacks and the data is not reliable. Data transmission using geographic routing is based on neighbor's node information. To avoid the problem, the author introduces the protocol known as Trust-based geographic routing protocol. Thus, the data delivery ratio improves up to 40%.Compared with existing work the proposed work is different in which redundancy is managed for intrusion/fault tolerance through multi-path routing using voting-based IDS to improve the lifetime of the network.

Jie Wang et al 2017 designed an improved clustering routing protocol (EDICP) based on energy and density by BEENISH protocol CH selection mechanism. The optimal CHs number is deduced according to the network energy consumption model, and the existing node density factor is modified. Then, the CH is selected according to the improved threshold formula. In the data transmission phase, the single-hop is used to transmit the data in the intra-cluster model. The CHs communicate with the BS using a single-hop and a hybrid way through a relay node. The simulation results show that the EDICP protocol reduces the energy consumption of the network and prolongs the network lifetime.

Purkar et al (2018) proposed to design an energy efficient clustering protocol for HWSN, to enhance performance parameters by EECPEP-HWSN. This protocol was designed with three level nodes namely normal, advanced, and super, respectively. In the clustering process, for selection of cluster head we consider different parameters available with sensor nodes at run time that is, initial energy, hop count, and residual energy. It enhances the energy efficiency of HWSN and thereby improves energy remaining in the network, stability, lifetime, and hence throughput. It has been found that the proposed protocol outperforms other existing well-known models like LEACH, DEEC, and SEP with about 188, 150, and 141 percent respectively.

3. Proposed method

3.1. Dynamic redundancy management algorithm

Dynamic management algorithm offers optimal redundancy by means of path redundancy (m_p) and source redundancy (m_s). Similarly, it also detects the intrusion by means of the number of voters (m) and the intrusion invocation interval TIDS to enhance MTTF (*Mean Time To Failure*), with respect to environment changes to input parameters including SN/CH node density, SN/CH radio range and SN/CH capture rate (λ_c).

3.1.1. Algorithm for cluster head execution

```
Initialization
Initialize the next task
Begin
If task is T_D timer then
find radio range to maintain CH
connectivity and also find optimal T_IDS, m_s, m_p
Notify to all sns about new Tids
Else if task is request message then trigger
multi-path routing
Else if task is Tclustering then perform
Tclustering
Else
Follow multi-path rouitng
End
Execute voting-based IDS
```

CH is elected based on radio range and also determine optimal path redundancy, source redundancy in accordance with the look up table [4,7]. This algorithm is based on the compromised rate of each node in the network. Around the CH, sensor node is considered as the voter. By voting based intrusion detection algorithm, it executes and finally the path has been chosen.

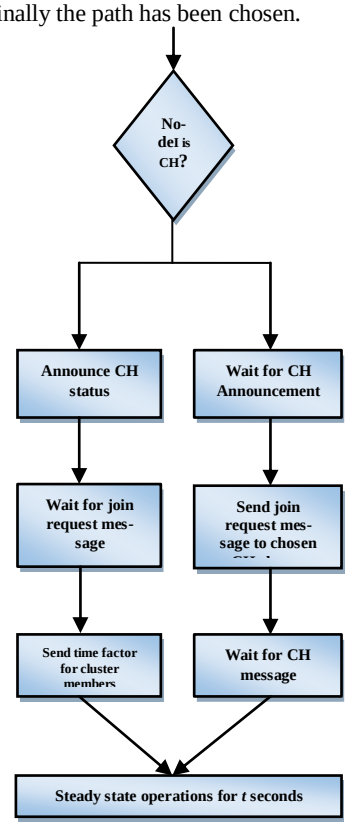

Fig. 3.1: Flowchart for CH Election Algorithm.

Figure 3.1. Represents the election of cluster head in the network. Consider the node *i* in sensor network. If *i* is cluster CH then broadcast the message to the neighbour sensor nodes, otherwise, the node *i* joins the CH by sending join message to the cluster. The number of cluster election algorithm is available to elect the CH. Here within the radio range and communication cost the CH is elected and trigger the multipath routing to initiate the task.

3.1.2. Algorithm for sensor node execution

```
Initialization
SN Execution
Get next task
Begin
If event is control packet arrival from CH
Then
Change the optimal settings of TIDS and m
Else if event is Tclustering timer then
Perform Clustering
End
For Each Neighbor SN
If Selected As a Voter Then
Execute voting-based intrusion detection
Else
Follow multi-path routing
```

The radio range of sensor node is elected and control packet is sent to the CH to form the cluster in reliable manner. And multi-path routing is triggered based on these optimal settings of the network. The timelineness is maintained by setting the *TIDS* timer. It also considers the energy level of each node to elect CH and sensor node. The above algorithm dynamically executes its action. Initially the radio range of CH connectivity is determined and the best m_p,m_s m,T_{IDS} are identified by lookup table which is based on the malicious node and radio range of cluster head. The optimal settings of T_{DS} is analyzed in each sensor node.CH accomplishes its tasks in the form of clustering according to the radio range for maintaining CH connectivity. Based on sensed environmental factors m_p,m_s,m,T_{IDS} are determined dynamically and SN_s are identified within the cluster of the new T_{IDS} and m settings. If the task assigns the network then it undergoes multi-path routing. Dynamic redundancy management algorithm in which execution cost is calculated in terms of periodic clustering, query processing, periodic intrusion detection, energy consumption. Overhead is eliminated due to periodic clustering.

3.2. Voting based IDS algorithm

The energy efficient IDS can be incorporated in sensor network by means of two approaches. The first technique takes care of flat WSNs. Here, it is essential for the intermediate node to forward reports on the maliciousness and energy status of the neighboring node to the source node which utilizes the details for sending packets free of malicious nodes in the network [6, 8, 10].The second technique which is employed in our study is local host-based IDS conserving energy where sensor nodes turn into monitor nodes at regular intervals. This approach is utilized to notify on compromised node in the sensor network.

3.2.1. Algorithm for voting based IDS

```
Initial
Determine neighbors within cluster range
(Snbr)Compute the thershold value for node
become compromised node
Begin
If v (monitor node) received the value
greater than threshold value than state as
"malicious node"
Else
the node become a member in a cluster
End
If CH receives m voters for a *nodethen it
sends data through the node
Else
The node is rejected in the network
```

4. Mathematical model

The energy consumed during the query and IDS with clustering interval is estimated by calculating total energy for the process. The energy exhausted for transmitting the data packet for length n_b bits by a sensor node is calculated as:

$$e_t = n_b(e_{elec} + e_{amp} r^x)$$

Where

e_{elec} is the energy utilized by the transmitter and receiver,

e_{amp} is the energy consumed for transmit amplifier,

R is the radio range of sensor network.

The energy utilized for receiving the message in a node is given by:

$$e_r = n_b e_{elec}$$

For processing the query i, $e_q(t_Q, i)$ is the total energy consumed for mp paths for the transmission between CH and PC which is represented by $e_q^{CH}(t_Q, i)$ .In similar way, for sensor node, it is represented as $e_q^{SN}(t_Q, i)$ .The total energy utilized for the transmission is as:

$$e_q(t_Q, i) = e_q^{CH}(t_Q, i) + e_q^{SN}(t_Q, i)$$

In conclusion, the energy consumed for implementing the clustering algorithm at time t_c,i, so the energy consumption is:

$$e_{clustering}(t_{c,i}) = N_{CH}(t_{c,i}) * e_T^{CH} + N_{SN}(t_{c,i}) * e_R^{SN} + N_{SN}(t_{c,i}) * e_R^{CH} + N_{SN}(t_{c,i}) * N_{SC}^{h}(e_T^{SN} + n_{SN}(t_{c,i}) e_R^{SN})$$

For intrusion detection, every node must evaluate the neighbor node through m voters, for that the energy spent is calculated as:

$$e_{ids}(t_{I,i}) = e_{ids}^{CH}(t_{I,i}) + e_{SN}^{ids}(t_{I,i})$$
$$e_{ids}^{CH}(t_{I,i}) = N_{CH}(t_{I,i-1})[m(m-1)][e_T^{CH} + n_{CH}(t_{I-i}) e_R^{CH}]$$
$$e_{ids}^{SN}(t_{I,i}) = N_{SN}(t_{I,i-1})[m(m-1)][e_T^{CH} + n_{CH}(t_{I-i}) e_R^{SN}]$$

From those equations, the energy utilized for clustering, ids and query processing is calculated and analyzed.

5. Result and discussion

5.1. Simulation parameters

Simulation parameters set for implementation and performance validation for simulation work. Some of those are explained as follows:

Stability period: The time period before the death of very first node from available sensor nodes of operating HWSN.

Number of alive nodes per cluster round: Number of nodes alive from the network for every cluster round, which indirectly presents the available energy remaining in the network.

Number of dead nodes per cluster round: Number of nodes dead per cluster round against changing energy level inside the network during network survival time. This factor indirectly presents death rate of nodes over cluster cycle. Which indicate possible lifetime remains with network in the form of cluster round.

Throughput: Number of data packets sent from the sensor nodes towards base station over the cluster round presents amount of throughput per cluster round. Amount of throughput signifies

energy efficient utilization of available network resources. Throughput presents quality of the network. The simulation factors represented in figure 5.1. as follows:

Serial Number	Parameter symbol	Name	Value
1	$M \times M$	Network area	200 m × 200 m
2	N	Number of nodes	200
3	E_0	Initial energy of nodes	0.5–1.5 J
4	L	Data packet size	4000 bits
5	E_{elec}	Radio electronics energy	50 nJ/bit
6	E_{efs}	Free space energy	10 pJ/bit/m^2
7	E_{mp}	Amplification energy	0.0013 pJ/bit/m^4
8	E_{DA}	Data aggregation energy	5 nJ/bit/signal
9	d_0	Threshold distance	87–87.7 m
10	BS	Sink node	(100, 100)

Fig. 5.1: Simulation Parameters.

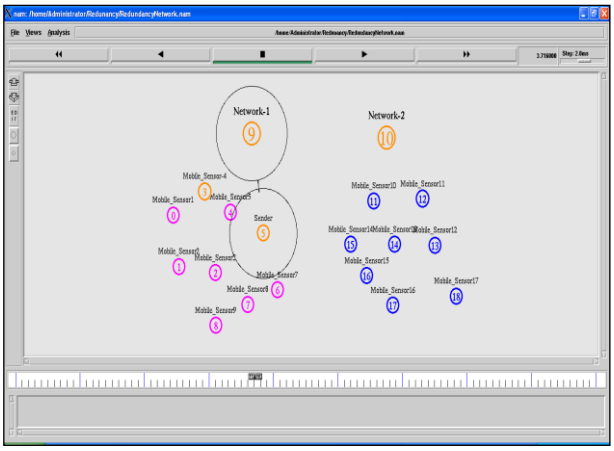

Fig. 5.2: Packet Transmission between Source and Destination.

Figure 5.2. Describes the sensor nodes are randomly deployed at initial stage, according to the radio range CH is formed. When the query arrived to the sensor node, it finds and sends the required data to sink. During the formation of CH, it considers the radio range and the communication cost among the nodes in the network.

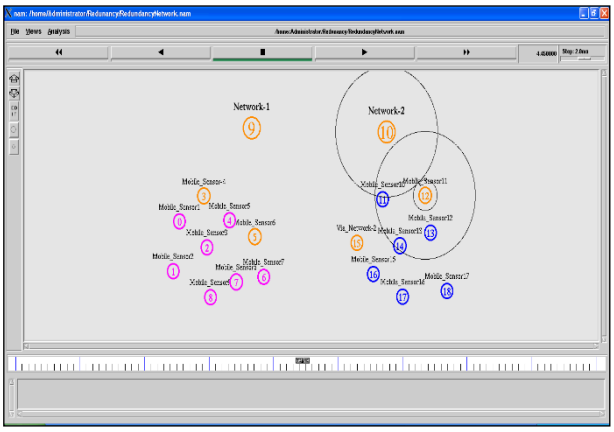

Fig. 5.3: Network 1 is Considered as Monitored Node for Neighbour CH.

Figure 5.3. represents the monitor node that is neighbor CH acting as a monitor node to detect the malicious node in the network. The source trusted to forward the sensed data is represented in pink color.

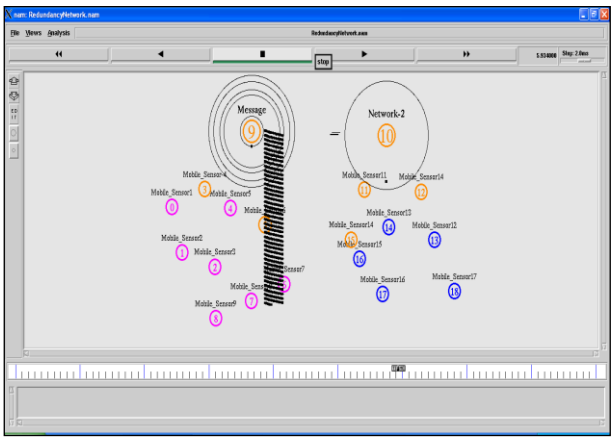

Fig.5.4: Packet Dropped Due to Malicious Node.

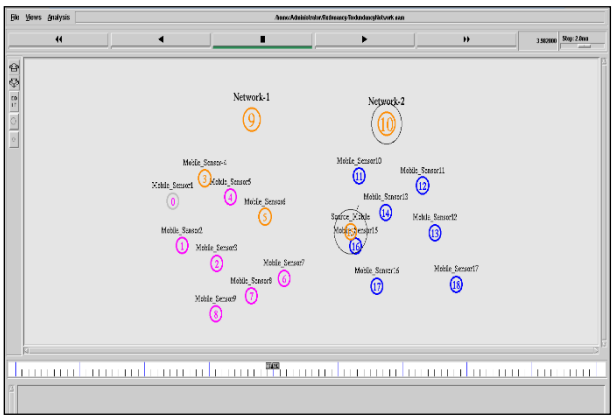

Fig. 5.5: Packet Sent to Sink in Reliable Manner.

Figure 5.4 and 5.5 explain about the packet dropped due to intrusions occurred in the system but path redundancy and source redundancy is managed through voting based IDS. So another secure path is available to send the same data in order to achieve high reliability. Dynamic redundancy management algorithm is used intend to reduce the packet dropping and other attacks.

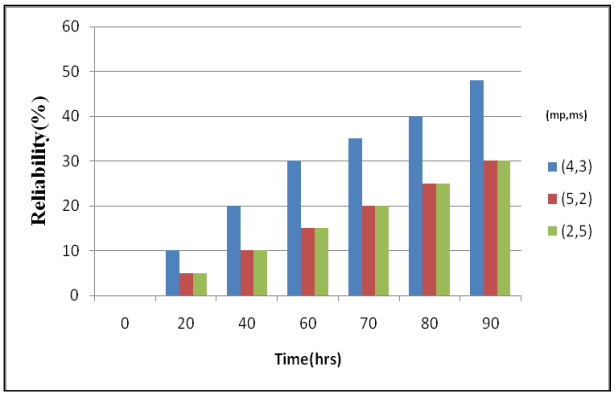

Fig. 5.6: Performance of Reliability.

Figure 5.6. represents the three combinations(m_s, m_p), in which (4,3) had the highest reliability due to high path and source redundancy. The reliability reached upto 49.87%. The data which has high source redundant as well as path redundant is reached the

high reliability. Security is also considered while sending data from source to sink.

6. Conclusion and future work

In this work, dynamic redundancy management algorithm is proposed to improve the lifetime of network. A novel probability model is to evaluate the optimal redundancy level in terms of path redundancy (m_p) and source redundancy (m_s). A voting-based IDS is useful to avoid the optimization problem through detecting the untrusted nodes in the network. By using the number of voters from the neighbor nodes, it detects the untrusted node. Security is also considered and it eliminates some of the attacks as bad-mouthing attack and packet dropping attack. Hence, from the analysis results, the algorithm achieves both QoS gain in reliability and security and also reduces the energy consumption.
In future, the work can be extended by considering the extensive attackers with different implications to security and reliability. Weighted voting algorithm can be used to strengthen the intrusion detection. At the same time, the traffic is also be reduced by using trust-based admission control algorithm.

References

[1] Akkaya K. and Younis M., "A Survey of Routing Protocols in Wireless Sensor Networks, " in the Elsevier Ad Hoc Network Journal, Vol. 3/3 pp. 325-349, 2005.

[2] Ammari H. M. and Das S. K., "Promoting Heterogeneity, Mobility, and Energy-Aware Voronoi Diagram in Wireless Sensor Networks," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 7, pp. 995-1008, 2008.https://doi.org/10.1109/TPDS.2008.31.

[3] Azad Azadmanesh, Alireza Farahani, and Lotfi Najjar, "Fault Tolerant Weighted Voting Algorithms International Journal of Network Security", Vol.7, No.2, PP.240-248, 2008.

[4] Bandyopadhyay S. and Coyle E. J., "An energy efficient hierarchical clustering algorithm for wireless sensor networks ", 22nd Conf. of IEEE Computer and Communications, pp. 1713-1723, 2003.

[5] Bao F., Chen I. R., Chang M., and Cho J., "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," IEEE Trans. Netw. Service Manga. vol. 9, no. 2, pp. 161-183, 2012.https://doi.org/10.1109/TCOMM.2012.031912.110179.

[6] Bhuse V. and Gupta A., "Anomaly intrusion detection in wireless sensor networks," J. High Speed Netw., vol. 15, no. 1, pp. 33-51, 2006.

[7] Bravos G. In addition, Kanatas A. G., "Energy consumption and trade-offs on wireless sensor networks," 16th IEEE Int. Symp. On Personal, Indoor and Mobile Radio Communications pp. 1279-1283, 2005.

[8] Chen.I.R. Speer.A.P. In addition, Eltoweissy.M. "Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks," IEEE Trans. on Dependable and Secure Computing, vol. 8, no. 2, pp. 161-176, 2011.https://doi.org/10.1109/TDSC.2009.54.

[9] Cheng S. T., Chen C. M., and Chen I. R., "Performance evaluation of an admission control algorithm: dynamic threshold with negotiation, "Performance Evaluation, vol. 52, no. 1, pp. 1-13, 2003.https://doi.org/10.1016/S0166-5316(02)00128-1.

[10] Cho J. H., Chen I. R., and Feng P. G., "Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks," IEEE Trans. Rel., vol. 59, no. 1, pp. 231-241, 2010.https://doi.org/10.1109/TR.2010.2040534.

[11] Dagon D., Qin X., Gu G. , Lee W., Grizzard J., Levine J., and Owen H., "Honeystat: local worm detection using honeypots," Recent Advances in Intrusion Detection. Springer, pp. 39-58, 2004.

[12] Deb B., Bhatnagar S., and Nath B., "ReInForM: reliable information forwarding using multiple paths in sensor networks," 28th IEEE Local Computer Networks, Bonn, Germany, pp. 406-415, 2003.

[13] Felemban.E.Chang-Gun.L.In addition,Ekici.E. "MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 5, no. 6, pp. 738-754, 2006.https://doi.org/10.1109/TMC.2006.79.

[14] Kang K. D., Liu K., and Abu-Ghazaleh N., "Securing Geographic Routing in Wireless Sensor Networks," ninth Annu. Cyber Security Conf. on Information Assurance, Albany, NY, USA, 2006.

[15] Jie Wang and Xue-ming Wang," An Improved Clustering Protocol for Energy Heterogeneous WSN", 2nd International Conference on Wireless Communication and Network Engineering (WCNE 2017) ISBN: 978-1-60595-531-5, 2017

[16] Santosh V. Purkar and R. S. Deshpande, "Energy Efficient Clustering Protocol to Enhance Performance of Heterogeneous Wireless Sensor Network: EECPEP-HWSN", Journal of Computer Networks and Communications,Vol. 2018,PP:1- 12.