NODE LEVEL ANOMALY MITIGATION THROUGH TRUSTWORTHY COMPUTATION BASED ELECTION OF FORWARDING NODES

M. GOWRI*, B. PARAMASIVAN[a]
Department of Information Technology, Sethu Institute of Technology, Kariapatti, India
[a]*Department of Computer Science and Engineering, National Engineering College, Kovilpatti, India*

This paper deals the detection of node level anomaly by calculating the trust value for each node. For the successful data transmission, it is necessary to select legitimate node. Novel trust computation mechanism has been devised for selecting next hop and it has been developed an enquiry based method to ensure secure communication. In WSN, each sensor node has its short transmission range. So the end to end communication among source to destination can be performed through multi hop communication. The existence of anomaly node may take over the control of packet forwarding during communication. The smooth functioning of the sensor network operations has been affected by the presence of anomaly node.

(Received May 24, 2017; Accepted June 29, 2017)

Keywords: Wireless Sensor Networks; Anomaly Detection; Intrusion Detection; Node Level Anomaly Detection

1. Introduction

Generally an anomaly node performs malicious activities that harmful to the network performance. Though number of attacks is confined, the conventional security solutions are unable to tolerate the wide range of vulnerabilities caused by the intermediate nodes during data transmissions.

The main aim of the proposed work is to provide resistance against the vulnerabilities by choosing trustable next hop for forwarding the data packets. The proposed Node level Anomaly Mitigation through Trustworthy computation based Election of Forwarding Nodes (NAMEFN) mechanism. NAMEFN provide better solution for the issues faced in existing schemes by increasing energy efficiency and reliability [1 – 5].

Since the WSNs communication is being done through the link that is often fluctuated in nature, it is not possible to achieve high reliability. This is not providing guarantee that the communication is not safe. Hence, it is necessary to determine the nodes that affect the data transmission and to maintain link between the intermediate nodes along with the communication path. The proposed NAMEFN mechanism considers the remaining energy and the quality of the link intermediate nodes involved in communication. Further, it selects the node with high quality of link and high residual energy as a forwarding hop during communication.

The proposed scheme resists the vulnerabilities caused by compromised intermediate hops in a multipath data transmission. This can be achieved by computing the trustworthy value for each intermediate hops in the communication path. Furthermore the proposed scheme augments enquiry based communication to ensure the security. This paper illustrates the design and development procedure of efficient packet transmission against denial of service attacks over the communication path [6 – 10].

*Corresponding author: vmkgowri@yahoo.com

The trust for each node can be determined based on the behaviour of the node in the previous communications. Trust is a well defined metric used to calculate the legitimateness of a node. The set of nodes are within the coverage area can communicated with each other each sensor can collaborate with each other to aggregate the sensed data and sent the aggregated data either to the Base Station (BS) or neighbouring sensor hops.

Before sending the sensed data, the route discovery has to be done. Generally sensor motes broadcast route request messages to find out active node around them and to establish the connection with it. Finding optimum route for data transmission is one of the issues faced in the route discovery process. But it is one of the most energy consuming processes in WSN. Hence it is necessary to select and prioritize the forwarding list to minimize the total energy cost of forwarding the data to the base station in wireless sensor networks.

The conventional route discovery mechanism provides solutions for finding shortest path or minimum hop count. They dealt the data forwarding process by considering the paths that posse's maximum residual energy or based on the quality of link. The existing schemes for routing are not suitable for ensuring reliable data transmission with considerable energy conservation. Cryptographic encryption and decryption algorithms and authentication schemes are not prevented the network from the damages caused by the intruders or adversary or malicious nodes. Regular monitoring process of nodes' behaviour is the only way to prevent the penetration of adversary node in data transmission.

In order to detect the existence of node anomaly in data transmission, it is necessary to monitor the behaviour of each node in the network. And it is also essential to calculate the trustworthy value for all nodes. Moreover, the life time and performance of the network can be increased by determining trust level based route discovery for transmitting the sensed data to the BS. The proposed system chooses the best next hop for forwarding the packet based on the trust value of each node. Each node's trust value can be determined by the past history of the node's communication and remaining energy of that node [11 – 15].

WSN is functioning as an intermediate medium between the physical environment and the computer system. The sensor nodes are sensing the physical phenomenon from the application area. The sensed data will be accumulated and forwarded to the base station. It is assumed that the sensors in the application environment are legitimate. The base station performs the appropriate decision after process the received data. The base station collected the data from the sensors by two ways. The one way is enquiry based data acquisition and the later one is collecting data periodically based on the event occurrence in the application area.

In enquiry based data collection, base station creates an inquiry and it will be routed towards the source node. The query related information is presented in the source node. Before routing the query message, the base station has to find a secure and reliable path. In addition, query message has to be protected from the path based denial of service attacks and false injection of data.

Most of the conventional false data detection schemes are used to protect the sensitive information against false data injection attack. In false data injection attack, an adversary injects false data through compromised intermediate hops in the en-route path. These schemes only detect false data by receiving the response message forward from source node.

But in enquiry based communication, it is necessary to protect the query request message and query response message. The proposed NAMEFN scheme is able to provide high security to the query request message and query response message. In this proposed system, the communication session key created by base station. That key is forwarded to the source node through authenticated neighbouring hops. In specific, the anomaly nodes are exempted for data forwarding. A hashed key chain method generated a key that has been used to authenticate forwarding node those are present in the communication path. The proposed scheme produces the optimal results over the existing schemes by identifying false data injection and early elimination of false report.

2. Proposed NAMEFN secure communication mechanism

In order to achieve reliable and secure data delivery, it is necessary to choose legitimate forwarding hops for data transmission. Since the WSN are deployed in unattended area, there is a high demand to provide security by prohibiting the involvement of anomaly nodes. The proposed NAMEFN scheme route the data packets in a specific communication path. This selection has been done based on the collected information from neighbouring nodes. The factors Quality of Link (QL) and Residual Energy (RE) are collected as information from the one hop distance neighbouring node. In the proposed scheme, periodically every node of the network has to determine its link quality with other nodes and remaining energy value. NAMEFN uses a forwarding node selection procedure for choosing a best en-route node. An authenticated and secure inquiry request and response based communication has also been augmented with the proposed system. The following section discusses the different stages of the proposed scheme (NAMEFN)

- Determination of link quality and residual energy
- Selection of trustworthy forwarding hop
- Authentication of en-route path
- Sharing of symmetric key
- Secure enquiry based communication

2.1. Determination of link quality and residual energy

Link Quality estimation schemes defines the quality of the link set up among two nodes. These techniques are also used for providing better connectivity to the network. Ensuring high connectivity between the nodes by resisting fluctuation results in reduction of dynamic topology changes in the network. In the proposed NAMEFN scheme QL values are treated as one of factors in the calculation of nodes' trust value. In specific calculation of QL factor is one of the deciding factors in the selection of forwarding hops. In order to determine the quality of the link, it is necessary to follow the three steps named monitoring the link, link measurement and link quality estimation.

Monitoring the link explains about the methods which are used for monitoring the traffic load for a link. It can be done in two ways active link monitoring and reactive link monitoring. Active link monitoring can be performed with the help of broadcasting or uni-casting the control packets that ensure the quality of the link between the pair of nodes in the network. Since this type of link monitoring increase the communication overhead, it is not suitable for WSNs. So the proposed scheme follows the reactive monitoring method. In this scheme each node monitors its traffic through the communications received within the time frame T_f. This calculation is being done without transferring the control packets.

Link measurement step is performed either by sender or receiver. In the proposed scheme receiver side are performing the link measurements. In order to do this, the receiver node uses the past history information about the successful communication. Here link measurements are calculated based on the successful reception rate of packets and its acknowledgements within the fixed time frame (T_f) and time interval (T_1 to T_2). The receiver node collects the details about the packets received within the time interval. Further, it collects the information about the packets sent through the sequence number specified in the received packets.

Algorithm for Link measurement

1. *Begin*
2. *Input: Data Packets from Sensor node within time interval T1 to T2*
3. *Initialise drop = 0, send = 0*
4. *Repeat*
5. *Extracts the sequence number from the data packet*
6. *If the sequence numbers are not continuous*

7. *drop++*
8. *else*
9. *sent++*
10. *Until Tf<T2*
11. *LM=sent/(sent+drop)*
12. *End*

In the proposed scheme NAMEFN, each node (source) intends to send a packet to its destination. Before data forwarding, residual energy of all possible neighbour hops will be calculated at each level. After deployment of WSN in an application specific area, each sensor node (SN_i) in the network is assigned with initial battery power E_i. During each network operation performed by a node, its remaining energy will be updated with a predefined time interval. The energy consumption of each node can be calculated as follows

$E(Tp)=E_{sen}+E_{Tx}+E_{Rx}$

E(Tp) is the energy consumption of a specific node during the time interval Tp which augments the energy needs for sensing, transmitting and receiving process. To the specific the energy requires for receiving and transmitting data packets depends on the size of the packet and the energy needed for run the electronics circuit to receive or transmitting n bits of packets. Equation () illustrates the remaining energy of a sensor node

RE(Tp)=RE(Tp-1)-E(Tp)

where RE(Tp) is the residual energy of a sensor Si in the time Tp, RE(Tp-1) is the residual energy during the previous updated time interval.

2.2 Selection of trustworthy forwarding hop

The proposed trustworthy forwarding hop selection procedure (TFHSP) chooses legitimate forwarding nodes for achieving secure enquiry based packet forwarding in WSN. When a base station aims to send a request message to collect the physical environmental information from a specified area using set of sensor nodes those are identified by its own unique name, it is essential to find an efficient path to the specified sensor node (S_id) which posses the event occurrence information. Hence, base station broadcasts a RREQ message. The RREQ packet includes the field of source address (S_id), destination address (BS_id). Once a one hop neighbour node receives the request message from the base station, it sent a RREP message to the base station. The RREP packet contains source address (S_id) and the destination address (BS_id) along with its residual energy value and quality of the link value.

After receiving RREP message from its one hop neighbour, the base station extracts the node information like residual energy, sensor node id and link quality value from the RREP message and those details are maintained using an array data structure named NOD-PROP-ARR. In addition, the base station uses two more other arrays to maintain the residual energy and link quality values separately in a sorted manner. As soon as routing is initiated by the base station, the TFHSP algorithm is invoked to determine the appropriate next forwarding hop to send the query request message. In order to attain optimal complexity for the proposed algorithm, higher priority information is retrieved from the sub-list maintained by the base station from the original array NOD-PROP-ARR.

After find out the sub-list, base station needs to choose an optimal pair of nodes with high link quality and maximum residual energy. Once the pair has been chosen, it is necessary to check whether the selected pair of node presents in the array NOD-PROP-ARR maintained by the base station. If the selected pair of node is not presented in the array NOD-PROP-ARR then it is necessary to select the next suitable pair of nodes and verify whether the selected pair exists in the NOD-PROP-ARR. If a suitable pair is not retrieved then selects the next higher priority sub-list. Once a suitable node is identified as per the proposed trustworthy forwarding hop selection algorithm, the same steps are followed to determine its next hop. This process will be repeated until the intended source sensor node (S_id) is reached. The intended sensor posses the required event information is reached. The detailed steps of TFHSP are listed as follows,

Step 1: Base station stores information like residual energy, sensor node id and link quality values received from one hop neighbour nodes in an array called NOD-PROP-ARR.
Step 2: Base station maintains two descending ordered arrays of size n named RE_Val[] and QL_Val[]. These arrays updated from NOD-PROP-ARR.
Step 3: Create sub-array RE_Val_S1[] from the sorted arrays RE_val[] with start index of the RE_val[] as begin index and (start index of the RE_val[]+Sizeof(RE_val[]))/2 as end index.
Step 4: Create sub-array QL_Val_S1[] from the sorted arrays QL_val[] with start index of the QL_val[] as begin index and (start index of the QL_val[]+Sizeof(QL_val[]))/2 as end index.
Step 5: Retrieve the maximum residual energy value and the highest link quality value obtained from the sub-arrays RE_Val_S1[] and QL_Val_S1[].
Step 6: If the retrieved node with the corresponding pair of value present in the array named NOD-PROP-ARR then do Step 7 otherwise repeat step 5 until the appropriate node retrieved from the sub -arrays
Step 7: Assume the retrieved node as the trusted next forwarding hop.
Step 8: If a relevant pair of maximum residual energy and link quality values are not obtained from the generated sub-arrays by do step 9 and step 10.
Step 9: Create sub-array RE_Val_S2[] from the sorted arrays RE_val[] with end index of the RE_val_S1 as begin index and (End index of the RE_val_S1[]+Sizeof (RE_val[ ]))/2 as end index.
Step 10: Create sub-array QL_Val_S2[] indexed from end index of the QL_val_S1[ ] as begin index and (end index of the QL_val[ ]+Sizeof(QL_val[ ]))/2 as end index.
Step 11: Repeat Step 5 to 10 until a pair of values relevant to the node in NOD-PROP-ARR is obtained. If such node is existed, that node must be treated as the trusted forwarding next hop. These steps are repeated until the selected node is an intended source sensor node with address S_id Authentication of en-route path

Once the destined sensor node receives the RREQ message, the authentication of en-route path has to be performed. In order to perform this, the destined sensor node initiates the process of generating and assigning a communication key (CK) to the forwarding nodes those are chosen by the TFHSP algorithm. Authenticate the nodes those are involved in the en-route path prevents the malicious activities of the anomaly nodes. The compromised forwarding nodes can pretend to be a selected for data transmission. The source sensor node 'S_id' distributes the CK to its selected one hop forwarding node. All other level forwarding hops obtain their CK from their ancestor upstream forwarding nodes. In addition the forwarding node is ensuring the integrity and validity of the query message transmitted from the base station through the communication key. The detailed steps to authenticate the en-route path are explained as follows.
Step1: The source sensor node 'S_id' calculates the CK through the hash function. The hase function uses the node address H(S_id) for calculating the CK. The hashed value will be sent as CK for its one hop forwarding node 'M'.
Step 2: Forwarding node 'M' receives and stores the CK from its upstream node. It further derives the CK by performs the XOR operation using two parametes H(M_id) with H(S_id). The generated key will be disseminated to next level forwarding nodes.
Step 3: The same process is repeated until base station receives the communication key from its upstream forwarding node.
Thus an authenticated en-route path that consists of trusted nodes ensure the detection of anomaly nodes and establish a secure path for data transmission.

2.3 Sharing of symmetric key

The base station sends a query message to the intended source sensor node. The main intension of sensing query message is to collect the details of particular event occurrence. In order to enhance the security level, it is aimed to provide next level protection to the query message by adopting cryptographic techniques. In the proposed scheme symmetric key based encryption technique is used to encrypt the query message which forward from base station to destined sensor node. This encryption scheme ensures that the encrypted query message can't be modified by any anomaly nodes in the network. The fields of the query request packets are query identifier (Q_id),

query request message, CK, timestamp (T_{stmp1}), encrypted symmetric key, secret key's integrity value. The procedure used for sharing the secret key is as follows

Step 1: Base station derives the details about the source sensor node from the CK disseminated from its upstream forwarding hop.

Step 2: Base station generates a symmetric secret key S_Sk and encrypt the S_Sk using the unique identifier of the destined node (S_id).

Step 3: Base station creates a secured packet that request the details about the event occurrence from the intended sensor node. The query request packet includes six fields named as query request message || CK || encrypted symmetric key ESK(S_Sk) || secret key's integrity value H(S_Sk) || T_{stmp1} || Q_id).

Step 4: Once the forwarding node receives the packet, it derives the CK from the received message to check the legitimacy of the packet. Then the retrieved CK is XORed with hash function of its ID and verified with its CK to check the legitimacy of the received message. If the match occurs, then the received message is authentic one. This process is repeated until the query message reaches the intended source sensor node.

Step 5: After gets the query request message, the source sensor node retrieves the CK and verifies the match with H(S_id). The packet is considered as valid one, if match occurs. Further it tries to decrypt the received encrypted packet using its identifier to retrieve the secret key. Then the validity of the retrieved secret key is verified using the integrity value stored along with the received encrypted message. If valid, that specified secret key can be used for future data transmission.

Thus the symmetric key based encryption scheme is prevented the involvement of the anomaly node in the routing process. This has been done by sharing the query request message and the secret key in a secured manner among base station and intended source sensor node.

2.4 Secure enquiry based communication

Once the intended source sensor node receives symmetric secret key and query request packet for the particular session, the source node initiates the process of sending query response message to the base station in a secured manner. The query response packet includes four fields communication key, query identifier, timestamp (T_{stmp2}), EK(query message)). The query report is sent to the base station. During enquiry based communication, it is important to verify the authenticity of query message which are received through the en-route path. The en-route path has the intermediate nodes. This helps to prevent the many attacks on the data transmission path. When the report arrives at next forwarding node, it retrieves the CK from the packet received and compares with the CK of its own. If it matches, then forward the packet by modifying CK of the next upstream forwarding node. This process continues until the packet reaches the base station. After receiving the packet the base station authenticates the packet using its CK. The time stamp value is used to checks the time of report generation. The base station is usually verify the freshness of the report and authenticates the query message using the field Query Identifier (Q_id). If the message is authenticated, then the base station decrypts the query response message using the key S_Sk for further processing. Thus the query response message is securely transmitted to the base station without intervention of any anomaly node.

3. Simulation and results

3.1 Study of Simulation Environment Setup

The proposed work is implemented in Network Simulator 2. The main aim of the experiment is to assess the performance of the proposed NAMEFN scheme with and without the involvement of anomaly nodes in the experimental setup. The simulated environment includes 500 nodes those are randomly deployed in 1000x1000m^2 area of interest. All sensor nodes are configured with homogeneous hardware and transmission power. The performance results are analysed by differing the number of nodes from 100 to 500 nodes. The simulation is tested in the presence of 5 to 30 anomaly nodes in the deployed network. The performance of the proposed

scheme in terms of security and reliability is compared with related schemes. The simulation parameter setup for this implementation is tabulated in Table 4.1.

Table 1. The simulation parameter setup for this implementation

Parameter	Value
Number of nodes	100,150, 200 and 500
Area of deployment (m^2)	1000 X 1000
Simulation Time (m)	120
Initial energy of each node (J)	10
Data Rate (Kbps)	100
Traffic Source	Constant Bit Rate
Propagation Model	Two Ray Round
Amount of energy needed to transmit one bit of information (nJ/bit)	60
Amount of energy spent for Amplification in Free Space Propagation ($pJ/bit/m^2$)	10
Amount of energy spent for Amplification in Multi Path Propagation ($pJ/bit/m^4$)	0.0013
Energy consumption for data aggregation (nJ/bit/signal)	5

3.2 Related works used for Comparison

The secure routing schemes by preventing the intervention of anomaly node in routing process (Chen 2007, Liu et al 2012 and Nasser & Zhan et al 2013) are taken for result comparison with the proposed schemes for evaluating the performance and security features.

The Trust-Aware Routing Algorithm for WSNs (TARA) (Zhan et al 2013) is chosen for performance analysis with the proposed secure routing scheme NAMEFN. TARA provided a trust based data transmission for WSNs against the presence of adversaries which performs malicious activities. The authors aim to provide trustworthy energy efficient route discovery for communication.

The proposed mechanism NAMEFN is highly resilient to misdirection routing attack performed by forging a valid node identity. The proposed mechanism is provided a better solution to address this issue by choosing trusted next hop for providing authenticated communication among intended source sensor node and base station. To enhance the security level of TARA, it is necessary to take the help of cryptographic algorithms to detect and drop compromised node communication. So there is a need of building a secure communication mechanism over TARA.

The existing algorithm called Energy-Efficient and Secure Disjoint Multipath Routing scheme for WSNs (EESDMR) (Liu et al 2012) is a three stage secret sharing scheme that sends the identical hop routes using least hop routing. The main aim of this scheme is to minimize the probability of eavesdropping and maximize network lifetime. By this algorithm, the authors have ensured that it highly impossible to decrypt the data packet by adversaries. The network security is increased by this scheme. The algorithm can extend the network lifetime, when the number of secret shares get reduced. The algorithm EESDMR increases the energy consumption thereby it reduces the network lifetime.

3.3 Discussions on Results Analysis

This section illustratesthe results analysis of the proposed secure NAMEFN communication scheme using simulation. The analysis refers the measures of trustworthiness and security of wireless sensor networks through the metrics network lifetime, delivery delay, probability of data delivery and the detection of false data injection. In order to evaluate the performance of the proposed scheme in an accurate manner, the experimentation is carried out by varying the number of anomaly node and varying the size of the network by changing the number of nodes from 100 to 500. Some outputs have been displayed with varyingthe size of network in the presence of only legitimate node and anomaly nodes. The metrics used for evaluation are defined as follows

Propagation delay: It can be described as the time required for a data packet to be sent from the source sensor node to the base station, including the route discovery and route maintenancetime duration.

Detection of False data Injection: It is a metric used fordetermining the efficiency of the proposed system in terms of security. It dealsthe probability of detecting false data injection of the proposed scheme. It can be calculated by the percentage of false data injection can be perceived by the en-route nodes based on their position of the source sensor node inthe presence of anomaly nodes.

Figure 1 shows the optimal performance in achieving network lifetime with varying the size of the network without the participation of any anomaly nodes. It has been found that network lifetime increases when the network size increased. When the network size is increased, the number of nodes participated in data transmissionalso gets increased. When the network consists of 200 nodes, the proposed system NAMEFN achieved the maximum (665 seconds(s)) network lifetime whereas EESDMR and TARA has network lifetime of 470s and 595s respectively.

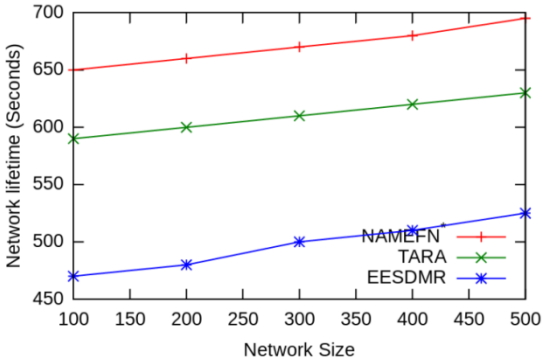

Fig. 1. Comparison of network lifetime with legitimate nodes

The proposed scheme found out the reliable link by calculating residual energy and link quality. The usage of such link prevents frequent link breakdown between source sensor node and destination nodes. Hence there is no need of performing retransmission which indirectly conserved the energy. Further, the lifetime of the network achieved by NAMEFN is 785s for 500 nodes and 630s, 525s for TARA and EESDMR respectively for the same network experimental setup.

Figure 2 shows the different level of network lifetime attainment in the presence of varying number of anomaly nodes in the network. In order to determine the mitigation level of anomaly nodes from the data transmission process, the network lifetime has to be observed by having 500 nodes as network size. And the same experiment has to be performed in the presence of 5 to 30 anomaly nodes among 500 network nodes. In the presence of 20 malicious nodes the network lifetime achieved by NAMEFN, TARA and EESDMR are 685s, 645s and 545s respectively. When the count of anomaly nodes increases, there is a need of sending the packet again to accomplish successful data transmission that indirect factor to affect the network lifetime.

The proposed NAMEFN is testedwith the participation of 5 to 30 anomaly nodes and noticed that the proposed scheme NAMEFN outperforms well even in the presence of anomaly nodeover other two related works. When the network consists of 30 number of anomaly nodes, the network lifetime of NAMEFN decreases to 645s. Likewise the increase in number of compromised nodes affect the lifetime of nodes in TARA and EESDMR.

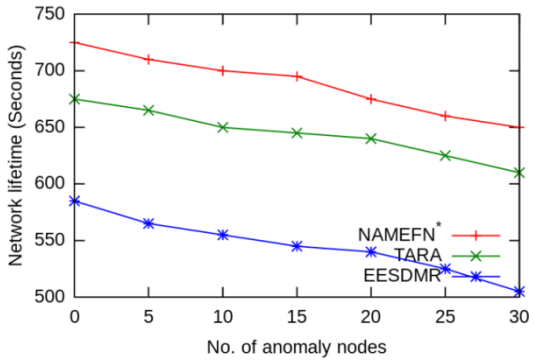

Fig. 2 Network lifetime in the presence of anomaly nodes

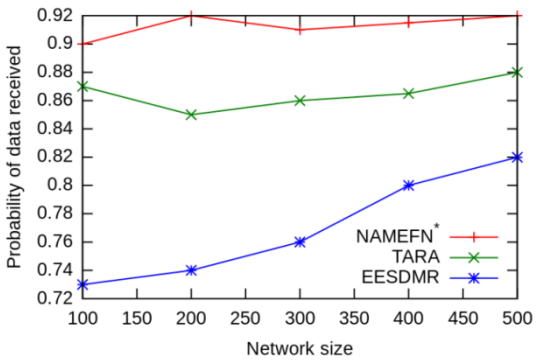

Fig.3 Probability of data received with legitimate nodes

Fig.3 shows the probability of successful data transmission when the network size is 500 legitimate nodes. Probability of successful data delivery can be measured by the number of data successfully received by the intended destination node over the total number of data sent by the source sensor node. It is observed that the proposed scheme NAMEFN scheme successfully delivered more number of packets to the destination than other two related works. When proceeds the experimentation with 300numbers of nodes the probability of data received by the destination node is 92% where as TARA and EESDMR achieves 85% and 74% of successful transmission ratio respectively.

Figure 4 explains the probability of successful data transmission in the presence of various levels of malicious nodes. From the simulation it is observed that NAMEFN achieves 82% of the data has been successfully delivered to the destination in the presence of 15 malicious nodes among 500 nodes in the simulated network. For the same simulation setup TARA and EESDMR shows 76% and 72% respectively. In the presence of 30 anomaly nodes NAMEFN outperforms 5% extra than TARA and EESDMR in successful data transmission to the destination. The main reason behinds the maximum performance of the proposed scheme is the selection of trusted path even in the presence of anomaly nodes in the network.

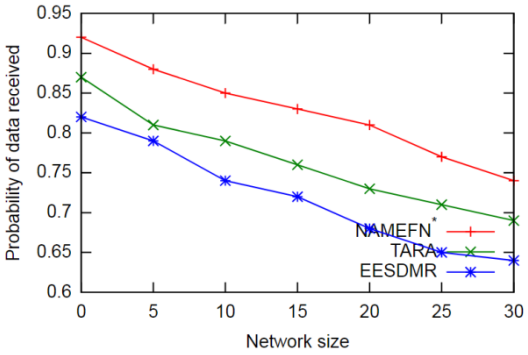

Fig.4 Probability of data received in the presence of anomaly nodes

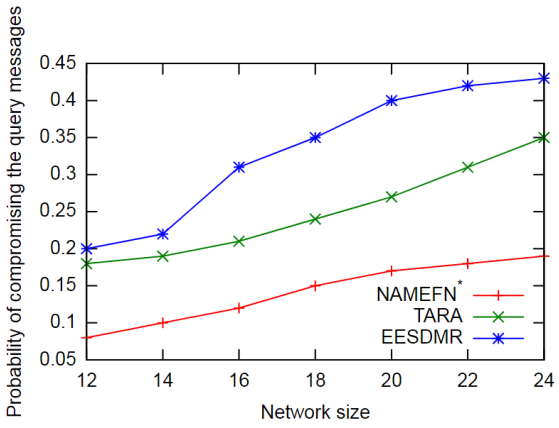

Fig.5 Analysing the chance for compromising the query packets

Security of the proposed scheme is based on the chance of protecting the query message from hacking and modifying the content of the query message by the adversaries or malicious or anomaly nodes. This performance analysis is illustrated in Figure 5.5. Simulation experiment is done by sending packets from a source sensor node to destination node. It also determines the how many number of packets modified by the adversary. The same simulation has been repeated by changing the hop count or varying the path length among the source sensor node and the base station. It has been observed that the proposed NAMEFN scheme shows the optimal performance (18% of packets only modified) when the path length is 22 whereas TARA and EESDMR modifies 31% and 36% of query messages. The main reason behinds the optimal performance of NAMEFN is key independence property and lack of key sharing probability among the neighbouring nodes of the en-route.

4. Conclusions

This paper proposes a fault tolerant, energy efficient routing mechanism for secure query based information transmission in a WSN. In this scheme the base station initiates the route discovery process. Base station initiated routing is more successful because the trusted entity initiates the route discovery process. This type of routing also prevents attacks on routing protocols that attracts traffic by advertising high quality routes. The proposed scheme overcomes the weakness of the previous schemes which consider energy alone as an important factor in performing route discovery operation. But the proposed scheme considers security along with energy which is very important for the success of many applications. Proposed scheme can achieve link layer security along with end to end security can protect query based communication from insider and outsider attacks. High network throughput can be achieved through proposed scheme

while the environment is free from compromised nodes due to high link-connectivity maintained in the nodes. Security analysis shows that the proposed scheme is highly resilient to false data injection attack and the replay attack that occurs in the path of message transfer while performing query based communication.

References

[1] R. Roman, J. Zhou, and J. Lopez, "On the Security of Wireless Sensor Networks", Proceedings of 2005 ICCSA Workshop on Internet Communications Security, pp 681-690, LNCS 3482, Singapur, May 2005.

[2] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications Anchorage, AK, May 11, 2003).

[3] A. D. Wood, J. A. Stankovic, Computer, 35**(**10), 54(2002).

[4] A. Perrig, J. Stankovic, D.Wagner, Communications of the ACM 47**(**6),53 (2004).

[5] A.S.K. Pathan, H-W. Lee, C. S. Hong, Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, Vol.2, 20-22 Feb. 2006

[6] S.Rajasegarar, et al. Anomaly detection in wireless sensor networks. IEEE Wireless Communications 15**,** 34(2008).

[7] V. J.Hodge, J. Justin,A survey of outlier detection methodologies. Artificial Intelligence Review **22**, 85(2004).

[8] V.Chandola,A.Banerjee, V. Kumar, Anomaly detection: A survey. ACM Comput.Surv. 41, 15 (2009).

[9] Yuan Yaoa, AbhishekSharmab, LeanaGolubchika,b, Ramesh Govindanb, Performance Evaluation 00,1 (2010).

[10] Raja Jurdak, X. Rosalind Wang, Oliver Obst, and Philip Valencia "Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies"/

[11] I. Solis, K. Obraczka, "In-Network Aggregation Trade-offs for Data Collection in Wireless Sensor Networks," INRG Tech. Report 102, 2003.

[12] N. Shrivastava, C. Buragohain, D. Agrawal, S. Suri, "Medians and Beyond: New Aggregation Techniques for Sensor Networks," ACM Sensys'04, pp. 239-249. New York, NY, 2004.

[13] C. Intanagonwiwat, D. Estrin, R. Govindan, J. Heidemann, "Impact of network density on data aggregation in wireless sensor networks," ICDCS, 2002, Vienna, Austria, pp. 457-458.

[14] S. Madden, M. J. Franklin, J. Hellerstein, Wei Hong, "TAG: a Tiny Aggregation Service for Ad-Hoc Sensor Networks," OSDI '02, Boston, Dec. 2002, pp. 131-146.

[15] J.-Y. Chen, G. Pandurangan, D. Xu, IEEE Transactions on Parallel and Distributed Systems, 17(9), 987(2006).