An Improved Malicious Data Injection Method and Secure Data Transmission in Wireless Sensor Network

Vandana Singh,
Technocrats Institute of Technology
and Science, Bhopal, M.P., India

Sudesh Gupta
Technocrats Institute of Technology
and Science, Bhopal, M.P., India

***Abstract* - A wireless sensor network comprises of several small sized sensor nodes that have computation capabilities. Consistency of WSN is affected by mistakes that may happen due to numerous reasons such as software malfunctions, malfunctioning hardware, dislocation, or environmental hazards. Error free and reliable data transfer between source and destination is the challenges in WSN. Malicious data injection plays a noteworthy role in network failure detection and network administration. Our technique enthusiastically detect the malicious data injection and immediately report to the system and perform data transmission with secure route. With the help of reverse route the node will send malicious data injection message to the upstream node. This error message is used by node to detect malicious data injection in the wireless sensor network. The standby node is used for transmission of secure data over WSN. Malicious data injection may cause failure of link in network. Malicious data injection plays a noteworthy contribution in network disaster detection and network management. This paper proposes a structure which automatically discover malicious data injection in node which may cause link failure and discover secure shortest path for data transmission. After detection of malicious data injection data can be securely transferred to the destination and improve the performance of wireless sensor network.**

Key-words: Wireless Sensor Network, WSN security, malicious data injection, Routing, Data transmission

INTRODUCTION

Associated to the wired networks, it seems considerable more important to sense malicious data injection rather than node responsibilities in WSNs.

A wireless sensor network comprises of several small sized sensor nodes that have computation capabilities. Wireless sensor networks (WSNs) have been widely used in many application areas such as infrastructure protection, environment monitoring and habitat tracing. Error free and reliable data transfer between source and destination is the challenges in WSN. Malicious data injection may cause failure of link in wireless sensor network. Our technique enthusiastically detect the malicious data injection and immediately report to the system and perform data transmission with secure route. Here verification framework is used to remove outside competitors and guarantee that only permissible nodes accomplish certain operations. The objective of our work is to detect malicious data injection in WSN, to determine route for protected data transmission. Malicious data injection plays a noteworthy role in network failure detection and network administration. Our technique enthusiastically detect the malicious data injection and immediately report to the system and perform data transmission with secure route. With the help of reverse route the node will send malicious data injection message to the upstream node. This error message is used by node to detect malicious data injection in the wireless sensor network. The backup node is used to secure data transmission.

Damaged link discovery plays an important part in network failure detection and network management. After detection of damaged link data can be securely transferred to the destination and improve the performance of wireless sensor network. The data transmission is possible only if like failure does not occur in wireless sensor network. In any circumstances if link down the network cannot continue to transfer the data to destination. With the help of reverse route the node will send link damage message to the upstream node. This error message is used by node to detect link failure in the wireless sensor network. This error message is used by node to change the protected and backup route for better data transmission. The backup route cache is fetched from the backup node to check link damage failure. This message is used by backup node to replace the contents of data packet. This packet is used to inform all the nodes about route changes in the network. After getting the message source node S directs the packets with new and secured node.

The rest of the paper is organized as follows.

Section 2 provides the background, relevant for the context. Section 3 provides the proposed methodology, proposed algorithm and description of proposed methodology. Section 4 represents the implementation of proposed methodology, discussion on simulation Results and performance analysis of simulation results. Section 5 concludes the paper with a summary of the main findings concluding remarks, limitation discussion and an outlook on future research directions.

II. BACKGROUND

A wireless sensor network comprises of several small sized sensor nodes that have computation capabilities. Wireless sensor networks (WSNs) have been widely used in many application areas such as infrastructure protection, environment monitoring and habitat tracing. Associated to the wired networks, it seems considerable more important to sense malicious data injection rather than node responsibilities in WSNs.

The battery is the main energy source in the wireless sensor network. For better performance battery power should be sufficient. Sensing unit consists of sensor and ADC (Analog to Digital Converter). Sensor senses the events and acts as an input for analog to digital converter. The analog to digital converter converts the analog signal into digital form. Then the output of sensing unit is input to the processing unit of wireless sensor network. Processing unit consists of microprocessor and memory. Microprocessor is the main component of processing unit. All the processing of wireless sensor network performed in microprocessor. Memory is used to store processing data and can be used for other related events. Communication unit is the unit used to communicate to the outside world.

The main WSN objectives are low node cost, small node size, low power consumption, scalability, self configurability, better channel utilization, fault tolerance, adaptability, Qos support and security. Therefore, error free and reliable data transfer between source and destination is the challenges in WSN. Consistent transfer of data is the surety that the packet carrying event's information reaches at the endpoint. The design challenges of WSN are limited energy capacity, sensor locations, limited hardware resources, massive and random node deployment, network characteristics and unreliable environment, data aggregation, diverse sensing application requirements, scalability.

Localization in wireless sensor networks is to fix the geographical locations of sensors in a WSN. The minimum solution is manual outline. The location of each sensor is planned before placement. Sensors are associated to the assigned locations by human. Obviously, solution is inscalable as much work is required for the installation. Furthermore, it is occasionally infeasible to have manual arrangement as the location information of sensors is anonymous before actual placement.

In WSNs, consistency can be categorized into diverse levels event or Packet dependability Level, End-to-End or Hop-by-Hop dependability Level

Nodes in WSNs are disposed to letdown due to hardware letdown, energy reduction, communication link faults, mischievous attack, and so on. Consistency of WSN is affected by mistakes that may happen due to numerous reasons such as software malfunctions, malfunctioning hardware, dislocation, or environmental hazards. Nodes in sensor networks have very limited energy. In ad-hoc network batteries can be replaced as and when needed. The battery condition of WSN node is very important factor for better communication. The hardware in good condition is very necessary for WSN communication. The communication of WSN is not only effected by antenna angle but also weather conditions, obstacles. It is also depends on interference.

Low-energy adaptive clustering hierarchy (LEACH): LEACH [36,37] is the first and most popular energy-efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption. The operation of LEACH is divided into rounds having two phases each namely (i) a setup phase to organize the network into clusters, CH advertisement, and transmission schedule creation and (ii) a steady-state phase for data aggregation, compression, and transmission to the sink.

LEACH is completely distributed and requires no global knowledge of network. It reduces energy consumption by (a) minimizing the communication cost between sensors and their cluster heads and (b) turning off non-head nodes as much as possible [38]. LEACH uses single-hop routing where each node can transmit directly to the cluster-head and the sink. Therefore, it is not applicable to networks deployed in large regions. Furthermore, the idea of dynamic clustering brings extra overhead, e.g. head changes, advertisements etc., which may diminish the gain in energy consumption.

III. PROPOSED WORK

OUR PROPOSED PROCEDURE CONTAINS SUBSEQUENT STAGES :

1) Initialization: During the *initialization*, the network is assumed to be free of compromise.
2) Pre-process the data to eliminate faulty readings, alleviate noise and transform the data to extract the parameters of interest
3) Check if the estimation models change in the presence of events, and if so we create a separate set of estimation models for each *modality* of the physical phenomeno
4) analyze the data to test if the correlation detected allows to build a linear model to perform the estimation,
5) the validity of a linear model is defined for each pair of sensors and allows to identify

the neighbourhood of as the set of sensors with which there is a strong linear relationship

(6) the parameters that fit the estimation models calculations.

(7) Secure node authentication

(8) Secure route discovery across the node.

```
    Select a node to destination
    Check selected node in fresh_route cache
If yes then
    Route is confirmed Else
        Select another new secured node
End if
```

(9) Backup node setup phase.

(10) Route maintenance across the node.

The first steps in algorithm is trust key value calculation. A novel parameter weight value named TLv can be used to select the finest track which guarantees reliability of the path by calculating the belief value of the adjacent nodes and that value can be stored in a precedence table of the scheme. Every time a node sends a route request either when it determines that it should be a part of a multi cast groups, and it is not already a member of that group, or when it has a message to send to the multi cast group but does not have a route to that group. An in-between node after receiving a route request packet updates its path in the routing table and add the TLv value of its link and forward it to the next node.

The next step is the route discovery. In this step the node will find secure node to transfer data from source to destination. We have used fresh route cache to easily find the path. Whenever data transmission phase is initiated the source node setup the route discovery phase and checks the fresh route cache to find destination nodes are available in the list. When source node found the routes are available in fresh route cache and node is authenticated then it conforms the process of data transmission. If the source node fails to find route in fresh route cache it will reinitiate the route discovery phase to probe for new secure node to the destination node.

The next step is backup node phase. Backup nodes are the nodes which contains the different secure path if the system fails to get the secure path. Due to backup node the data can be transferred to destination. When route discovery request along with the route cache confirm reaches the destination D, it may collect different secured routes with in a period.

The destination D received all the paths of nodes. All the paths are collected and compared to check whether any two route are common. The backup node is defined as the node containing all common node collecting from nodes excluding destination D. A subdivision of backup nodes can be collected from any two protected routes.

The next step is to maintain the route for secure data transmission. Damaged link detection becomes more problematic in the multi-hop networks due to topology structures. Damaged link discovery plays an important part in network failure detection and network management. After detection of damaged link data can be securely transferred to the destination and improve the performance of wireless sensor network. The data transmission is possible only if like failure does not occur in wireless sensor network. In any circumstances if link down the network cannot continue to transfer the data to destination. With the help of reverse route the node will send link damage message to the upstream node. This error message is used by node to detect link failure in the wireless sensor network. This error message is used by node to change the protected and backup route for better data transmission.

The backup route cache is fetched from the backup node to check link damage failure. This message is used by backup node to replace the contents of data packet. This packet is used to inform all the nodes about route changes in the network. After getting the message source node S directs the packets with new and secured node.

IV IMPLEMENTATION

We used NS2 simulator for implementation of proposed work. We also used C/C++ and TCL language for implementation. We performed our experiment in PIV 2.0 GHz machine with 2GB RAM. In our simulation work, we have different the amount of nodes from 50 to 300, which are arbitrarily positioned in dissimilar parts of positioning part with a static density. For this simulation, we have used the network parameters, such as Dimension, Number of nodes, traffic, transmission rate, Routing protocol, transmission range, sensitivity, transmission power etc., are used. We have performed our experiment with different number of nodes, with or without mobility. The dimensional area and speed of the scenario is also changed according to situation. With the help of reverse route the node will send link damage message to the upstream node. This error message is used by node to detect link failure in the wireless sensor network.

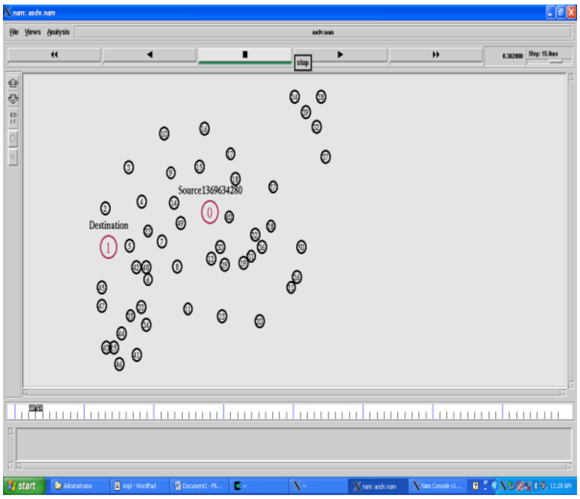
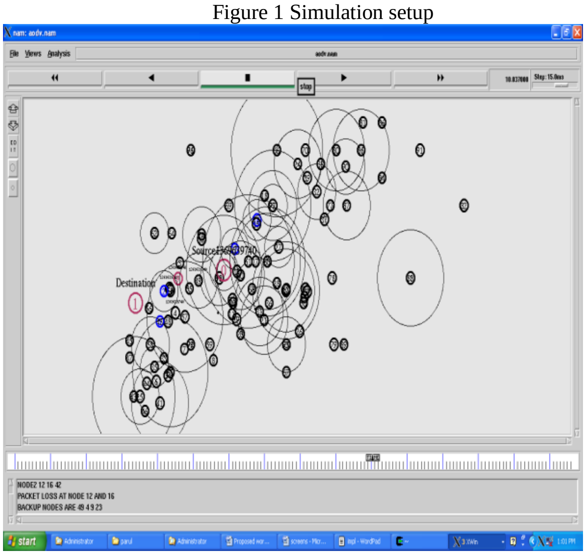


Figure 1 Simulation setup



```
NODE2 12 16 42
PACKET LOSS AT NODE 12 AND 16
BACKUP NODES ARE 49 4 9 23
```

Figure 2 Simulation result

Simulation readings of the proposed protocol are carried out to estimate its performance, and compared its performance. Fig. 2 represents the data transfer percentage of all the three routing protocols. It is noted that the data transmission ratio of all the set of rules rise as the node compactness increases. When node density is very high, there are additional nodes available for data promoting, and this rises the delivery ratio.

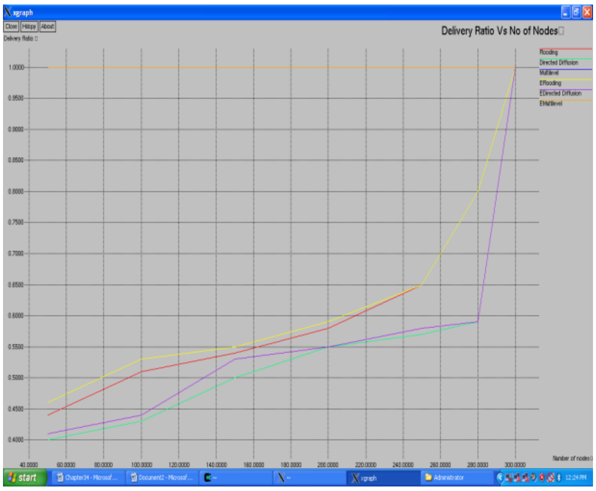


Figure 3 Performance Graph for Delivery Ratio Vs Number of Nodes

Table 1 Simulation scenario

Quantity of nodes	50, 100, 150, 200, 250, 300
Simulated area dimension	810×610
Routing Procedure	LEACH
Simulation time in seconds	110
Transport Layer	FTP, TCP
Traffic flow type	CBR
Packet size in bytes	1010
Quantity of traffic links	20 , 8
Max. Speeds in m/s	30

Fig. represents the data transfer percentage of all the three routing protocols. It is noted that the data transmission ratio of all the set of rules rise as the node compactness increases. When node density is very high, there are additional nodes available for data promoting, and this rises the delivery ratio. Overflowing offers less data delivery rates, followed by flooding is directed diffusion; it did not familiarize well its performance to network size growth. The multilevel routing protocol has preserved continuous transport rates throughout the simulated situations. This is an outcome of the influence of the process it uses to create a routing route.

V. CONCLUSION

Malicious data injection plays an important part in network failure detection. It is also used in network administration. Associated to the wired networks, it seems considerable more important to sense malicious data injection rather than node responsibilities in WSNs. After detection of malicious data injection data can be securely transferred to the destination and increase the enactment of wireless sensor network. Malicious data injection may cause failure of link in wireless sensor network. A wireless link itself nearly exists, which means we can't directly see and appraise whether it achieves well or not. It demonstrates problematic to localize the broken-down links under a dynamic mal-condition in the remote, for the link quality will be meaningfully impacted by the natural environment like flow in the ocean and trees in the forest. Malicious data injection discovery becomes more difficult in the multi-hop networks due to topology structures. Malicious data injection detection plays a noteworthy role in network failure detection and network administration. Our technique enthusiastically detect the malicious data injection and immediately report to the system and perform data transmission with secure route. This paper proposes a structure which automatically discover malicious data injection in node which may cause link failure and discover secure shortest path for data transmission. After detection of malicious data injection data can be securely transferred to the destination and improve the performance of wireless sensor network.

REFERENCES

[1] Vittorio P. Illiano and Emil C. Lupu, Detecting Malicious Data Injections in Event Detection Wireless Sensor Networks, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 12, NO. 3, SEPTEMBER 2015, pp-496-512

[2] T. S. Rappaport et al., Wireless Communications: Principles and Practice, vol. 207, Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.

[3] W. Dong, Y. Liu, Y. He, T. Zhu, and C. Chen, "Measurement and analysis on the packet delivery performance in a large-scale sensor network," IEEE/ACM Trans. Netw., vol. 22, no. 6, pp. 1952–1963, Dec. 2014.

[4] H. Chang et al., "Spinning beacons for precise indoor localization," in Proc. ACM SenSys, Raleigh, NC, USA, 2008, pp. 127–140.

[5] Qiang Ma, Kebin Liu, Zhichao Cao, Tong Zhu, Yunhao Liu, Link Scanner: Faulty Link Detection for Wireless Sensor Networks, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 14, pp 4428-4438, Aug 2015

[6] S. S. Ahuja, S. Ramasubramanian, and M. M. Krunz, "Single-link failure detection in all-optical networks using monitoring cycles and paths,"
IEEE/ACM Trans. Netw., vol. 17, no. 4, pp. 1080–1093, Aug. 2009.

[7] Q. Cao, T. Abdelzaher, J. Stankovic, K. Whitehouse, and L. Luo, "Declarative tracepoints: A programmable and application independent debugging system for wireless sensor networks," in Proc. ACM SenSys, Raleigh, NC, USA, 2008, pp. 85–98.

[8] A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D. Estrin, "Statistical model of lossy links in wireless sensor networks," in Proc. IEEE IPSN, 2005, pp. 81–88.

[9] L. Girod et al., “EmStar: A software environment for developing and deploying wireless sensor networks,” in Proc. USENIX Annu. Tech. Conf., Boston, MA, USA, 2004, p. 24.

[10] Y. Hamazumi, M. Koga, K. Kawai, H. Ichino, and K. Sato, “Optical path fault management in layered networks,” in Proc. IEEE GLOBECOM, Sydney, NSW, Australia, 1998, pp. 2309–2314.