Reducing the gang injecting false data attack from compromised Sensor nodes using random graph and bit compressed Authentication techniques

[1].A. Mallareddy, [2] P.Keerthi, [3] D.Prathibha

[1]Research Scholar(JNTUH), Department of Computer Science & Engineering, Professor & HOD(CSE)

[2]M.Tech (CS) , Department of Computer Science,

[3]Associate Professor, Department of Computer Science & Engineering, Sri Indu Institute of Engineering & Technology, Sheriguda(V), Ibrahimpatnam(M), RR Dist – 501510.

ABSTRACT

In wireless networks data will be send in terms of packet, while forwarding data from one end to another end by using sockets there having a chance of attacks like denial of service. The Sink node verifies every packet with MAC (Message Authentication Code) if the Timestamp is valid else drop the packet. As the sink is verifying every packet it causes the bottleneck at the sink, to avoid this problem we are introducing BVFG scheme for filtering and reducing the gang injecting false data attack from mobile compromised sensor nodes using random graph and bit compression authentication techniques, with this the injected false data can be filtered by En- Routes. With this we can effectively find the node which is not injected by false data. The proposed BVFG will provide us efficiency, best filtering probability, reduced overhead and time of verification.

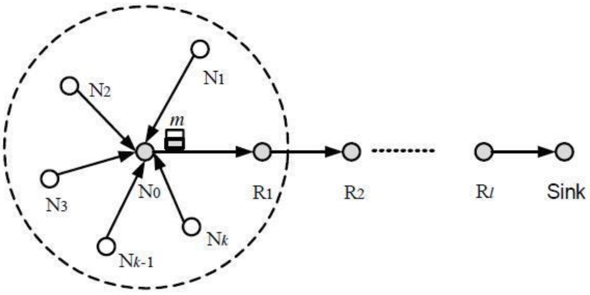
Index Terms:- Wireless Sensor Network, False Data Injection, Gang Data injection, Management of Energy Waste, Bit Compression

1. INTRODUCTION

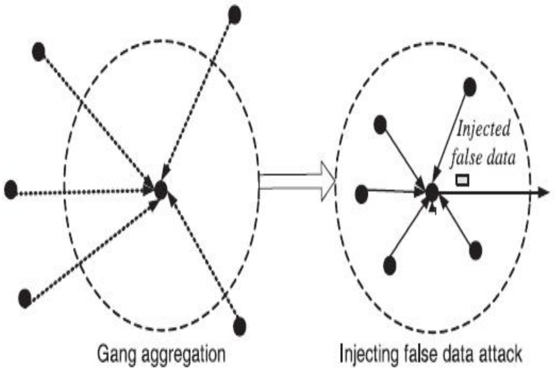
In networking sending data over the network is a part of digitalization. While forwarding data over the networks there having a chance of attacks like denial of service, brute-force attack. This section first presents the architecture of a WSN. Next the coordinator selection methods are presented. The routing model used in this study is then presented. A wireless sensor network consists of large number of sensor nodes to perform allotted sensing tasks by interlinking with wireless nodes [1]. Every sensor is affordable and it has required components to sense, process data, and to maintain communication with other sensors. In every wireless network a collection unit will be maintained and it is known as SINK. It receives every report which will be generated by the sensors through En-Route nodes. In wireless sensor network, the sensor nodes are established at uncongenial environments. In such environments sensor nodes are in-secured and week, so that it causes several kind of attacks like false data injection, selective forwarding wormholes and Sybil attacks more chances to inject false data by compromising the en-route nodes. In our paper we are proposing batch verification scheme for reducing the gang injecting false data attack from mobile compromised sensor nodes using random graph and bit compression authentication techniques, with this the injected false data can be filtered by En- Routes. When the sender sends the injected response to the receiver, with the proposed scheme we can filter the data at every sensor node with the MAC (Message Authentication Code). Whenever the response reaches the node it will check for timestamp validity, if it is valid then verifies the MAC and forward response to another en-route, else it will drops packet and blocks the compromised node.

2. EXISTING METHODOLOGIES

In existing technologies sensor node detects all neighbour nodes including the neighbour sensor nodes and forwarding nodes. Once it detects all neighbour nodes, depending upon the mobility of the sensor node, cluster head will be chosen. The sensor node, which has high mobility, acts as a cluster head. . The sink is one of the most powerful data collecting device which has sufficient computation and storage capabilities and is responsible for initializing the sensor nodes and collecting the data sensed by these nodes. But in over scheme, we assume Sensor node transmits sensed data to cluster head, cluster head then forwards to the source.



Architecture of Existing System



Gang Injection of false data

3. PROPOSED SYSTEM

The filtering probability at each en-routing node is relatively low. Besides, SEF does not consider the possibility of en-routing nodes' compromise, which is also crucial to the false data filtering.

A. Hop-by-hop authentication (IHA)

Zhu et al. presented an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data. In IHA, each node is associated with two other nodes along the path, 1.Lower association node, and 2.Upper association node. An en-routing node can forward the received report if it is successfully verified by its lower association node. To reduce the size of the report, the scheme compresses individual MACs. The security of the scheme is mainly contingent upon the creation of associations in the association discovery phase. Once the creation fails, the security cannot be guaranteed. The symmetric keys from a key pool which allows the compromised nodes to misuse these keys to generate false reports.

B. Location-Based Resilient Secrecy (LBRS)

Yang et al. proposed Location-Based Resilient Secrecy (LBRS), which adopts location key binding mechanism to reduce the damage caused by node compromise, and further mitigate the false data generation in wireless sensor networks. To achieve en-routing filtering, authentication overheads are required additional 20 bytes.

C. Location-aware end-to-end data security design (LEDS)

Location-aware end-to-end data security design (LEDS) Ren et al. propose more efficient location-aware end-to-end data security design (LEDS) to provide end-to-end security guarantee including efficient en-routing false data filtering capability and high-level assurance on data availability. To achieve en-routing filtering, additionally 20 bytes authentication overheads are required. It assumes that all the nodes can determine their locations and generate location-based keys in a short secure time slot.

D. Public key based solution.

Zhang et al. provide a public key based solution to the same problem. Especially, they propose the notion of location-based keys by binding private keys of individual nodes to both their IDs and geographic locations and a suite of location-based Compromise-tolerant security mechanisms.

E. Bit-compressed authentication technology

Bit-compressed authentication technology can achieve bandwidth-efficiency. Canetti et al. use one-bit authentication to achieve multicast security.

Diagram:

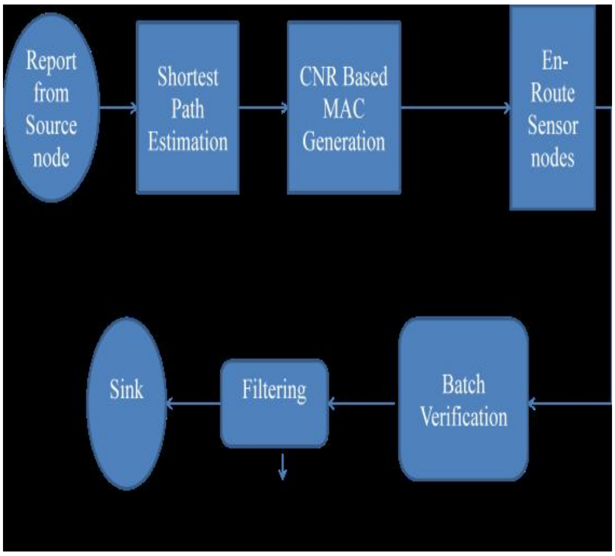


Fig: Block Diagram of Procedure.

4. MODULE DESCRIPTION

A. Sensor Node Initialization:

The sink deploys these initialized sensor nodes at a Certain Interest Region (CIR) in various ways, such as by air or by land. It is assumed that all sensor nodes are uniformly distributed in CIR after deployment. When these sensor nodes are not occupied by the reporting task, they cooperatively Establish or adjust their routing to the sink either a shortest path or a path adapted to some resource constrains with some existing routing protocol. Note that, the established routing path can accelerate the reporting. Once an event occurs, a report can be immediately relayed along the established routing path.

Steps of Module Description

Step: 1 Create a Base station in cluster 1.
Step: 2 create two forwarding nodes in Cluster 1 and cluster 2.
Step: 3 create two sensor nodes in cluster 1.
Step: 4 Base station, Forwarding node and sensor Nodes will have a unique identity Let sensor Nodes N= {N0, N1, N2...}.
Step: 5 establish a key pool containing various random generated key values.
Step: 6 initialize each sensor node with a key
value from the key pool.

B. Routing establishment

In the proposed model, base station, forwarding node and sensor nodes has been designed. Base station receives message from sensor node. While establishing sensor node, the system identifies the cluster head, which is also one of the sensor node. Sensor node always sends data via cluster head, then to forwarding node and then to base station. For this sensor node and forwarding nodes must establish their neighbour nodes automatically.

C. Sensed results reporting

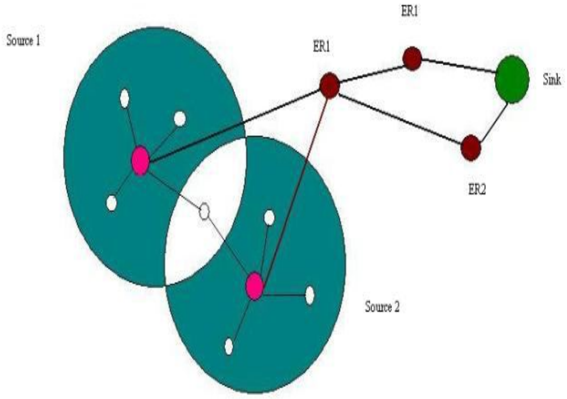
When a sensor node generates a report m after being triggered by a special event, e.g., a temperature change or in response to a query from the sink, it will send the report to the sink via an established routing. Assume that, the sensor (source) node NO has sensed some data m and is ready to report m to the sink via the routing path R N0: {RI - R2 . . . R - Sink}. The source node NO gains the current timestamp T, chooses k neighbouring nodes N N0: {N1, N 2, . . ., N k} and sends the event m.

D. CNR Based MAC Generation

To filter the false data injected by compromised sensor nodes, the E-BCA scheme adopts cooperative neighbour router (CNR)-based filtering mechanism. In the CNR-based mechanism, when a source node NO is ready to send a report m to the sink via an established routing path RNO: {Rl - R2 . . . Rl- Sink}, it first resorts to its k neighbouring nodes NNO :{N1,N2, . . .,Nk} to cooperatively authenticate the report m, and then sends the report m and the authentication information MAC from NO to the sink via routing RNO, where the sink initializes all sensor nodes, then each sensor node shares it.

5. EXPERIMENTAL RESULTS

Filtering the false injected data is the main problem in wireless sensor network. The E-BCA scheme is used to filter the false data by verifying the unique MAC of every node. We consider the implementation of a Base Station, two Forwarding Nodes and two Sensor Nodes. Base Station is created in cluster l and the Certain Interest Region (CIR) value is 1. First Forwarding node in cluster l and region value is 100. Second forwarding node in cluster2 and region value is 70. Similarly, two sensor node in cluster l. Mobility value of sensor node is read by percentage value. The node, which is having high percentage, is considered to be the cluster head. Each sensor node acquires a key pair value form keys, properties file and data for forwarding is taken from sensor properties file. We design attackers in two forms, one is for giving wrong time value and another is for giving wrong key input. Sensor node first forwards the data to cluster head. Cluster head forwards to forwarding node. The filtering of false data is carried out in forwarding node. Once the forwarding node gets data from cluster head, it checks the received data, which contains a message, key pair, MAC key and timestamp. There are two conditions are checked as attacker. One is when the forwarded data contain old timestamp it is considered to be false data attack. Another one is, when the forwarded sensor node's key is not matched with key pool value, and then it considered as the attacker. As the detection of attacker is identified in the earlier stages, that is, it is identified in the forwarding node itself and not in the base station, thus our application considered to be bandwidth efficient.



Batch Verification with En-route filtering

6. CONCLUSION

In this paper, we have proposed a novel E-BCA scheme for filtering the injected false data. By theoretical analysis and simulation evaluation, the E-BCA scheme has been demonstrated to achieve not only high filtering probability but also high Reliability and multi reports on time out basis and key management basis and it easily find out the gang injection false data attack. Due to the simplicity and effectiveness, the E- BCA scheme could be applied to other fast and distributed authentication scenarios, e.g., the efficient authentication in wireless mesh network.

7. FUTURE ENHANCEMENTS.

In Future work it may be investigate how to prevent/mitigate the gang injecting false data attack from mobile compromised sensor nodes. Consider the scenario, when the wireless sensor node moves from one location to another location, it is difficult to identify the false data injection through this proposed mechanism.

REFERENCES

[1] R.Szewczky, A. Mainwaring, J. Anderson, and D. Culler, "An Analysis of a Large Scale Habit Monitoring Application," Proc. Second ACM Int'l Conf. Embedded Networked Sensor Systems (Sensys '04), 2004.

[2] L.Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), 2002.

[3] R. Lu, X. Lin, C. Zhang, H. Zhu, P. Ho, and X. Shen, "AICN: An Efficient Algorithm to Identify Compromised Nodes in Wireless Sensor Network," Proc. IEEE Int'l Conf. Comm. (ICC '08), May 2008.

[4] X. Lin, R. Lu, and X. Shen, "MDPA: Multidimensional Privacy- Preserving Aggregation Scheme for Wireless Sensor Networks," Wireless Comm. and Mobile Computing, vol. 10, pp. 843-856, 2010.

[5] X. Lin, "CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks," Proc. IEEE GLOBECOM '09, Nov.-Dec. 2009.

[6] K. Ren, W. Lou, and Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," Proc. IEEE Sensor Ad Hoc Comm.Networks (SECON '07), June 2007.

[7] L. Zhou and C. Ravishankar, "A Fault Localized Scheme for False Report Filtering in Sensor Networks," Proc. Int'l Conf. Pervasive Services, (ICPS '05), pp. 59-68, July 2005.

[8] Z. Zhu, Q. Tan, and P. Zhu, "An Effective Secure Routing for False Data Injection Attack in Wireless Sensor Network," Proc. 10th Asia-Pacific Network Operations and Management Symp Mobile compromised sensor nodes (APNOMS '07), pp. 457-465, 2007.

[9] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM '04, Mar. 2004.