ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014

International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

Detection and Elimination of False Data in Wireless Sensor Networks for Efficient Utilization of Bandwidth

Vrinda R[1], Bharathi M A[2]

M.Tech Student, Dept of Computer Science, Reva Institute of Technology and Management, Bangalore, India[1]
Associate Professor, Dept of Computer Science, Reva Institute of Technology and Management, Bangalore, India[2]

ABSTRACT: Wireless Sensor Networks are usually deployed at the hostile environments. So they are vulnerable to injecting false data attack. An adversary could compromise one or more sensor node and access all stored materials then inject the false data which causes energy wasted in en-route. In this paper, Detection and Elimination of False Data in Wireless Sensor Network for Efficient Utilization of Bandwidthscheme has been proposed. This scheme can save energy by detecting and filtering the injectedfalse data with less time and difficulty at the en-route nodes. In addition,only a small amount of injected false data needs to be checked by the sink, this reduces the burden on sink.

KEYWORDS: Injected false data,Wireless sensor network, compromised sensor node, sink

I. INTRODUCTION

A wireless sensor network is usually composed of a large number of sensor nodeswhich are interconnected through wireless links to perform distributed sensing tasks. Each sensor node consists of data sensing, processing, and communicating components. When sensor node generates a report on event, e.g., atemperature change at surrounding will send a report to the data collection unit, sink through an established routing path.Wireless sensor networks are usually deployed at environments which are more vulnerable to various security attacks, the most serious and dangerous one is injecting false data attack. For this injected false data attack, first several sensor nodes are compromised by an attacker, then attacker accesses all keying materials stored in compromised nodes, process it and send the false data to the sink. One disadvantage of this attack is large number of expensive resources will be wasted. Therefore, filtering the false data is a crucial process and it should be accurate in wireless sensor networks.Simultaneously all the false data injected are flooding into the sink, heavy verification burden will fall on the sink, and huge energy will be wasted at the en-route nodes in the established path. Therefore, it is must to filter false data faster and earlier as much as possible in a tactful way to mitigate the energy waste at the en-route nodes and sink. Some false data filtering mechanisms have been developed to tackle this issue. These existing filtering mechanisms use the symmetric key technic. The problem with it is the attacker can take an advantage of compromised node keys to generate false reports. Therefore, reliability of such filtering mechanisms will be degraded. Where the proposed mechanism, Detection and Elimination of False data in Wireless Sensor Network for Efficient Utilization of Bandwidth resolves this problem by early detecting and filtering the false data, hence saves theenergy. The sink needs to verify a very small amount of injected false data, thus reduces the burden of the sink. Compare to previous mechanisms, this new mechanism achieves maximum filtering probability and high reliability.

II. EXISTING SYSTEM

Different works on filtering of injected false data in wireless sensor networks for efficient utilization of bandwidth have been appeared using message authentication code, key binding mechanism and bit compression authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014

International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

A. Statistical En-route Filtering(SEF)

Statistical En-route Filtering (SFE) requires that each sensing report be validated by multiplekeyed message authenticated code, each generated by a node that detects the same event. As the report being forwarded, each node along the way verifies the correctness of the MACs at earliest point. If the injected false data escapes the en-routing filtering and is delivered to the sink, the sink will furtherverify the correctness of the each MAC carried in each report and reject false ones.

B.Interleaved Hop by Hop Authentication

Interleave-hop-by-hop authentication (IHA) scheme for filtering of injecting false data, which each node is associated with two other nodes along the path, one is the lower association node, and other is the upper association node. Anen-routing node will forward,received report if it is successfully verified by its lower association node.

C. Location Based Resilient Secrecy

Location-Based Resilient Secrecy (LBRS) adopts location key binding mechanism to reduce the damage caused node compromise, and further mitigate the false data generation in wireless sensor networks.

D.Location Aware End to End Data Security Design (LEDS)

Location-aware end-to-end data security design(LEDS) provide end-to-end security guarantee including efficient en-routing false data filtering capability and high level assurance on data availability.LED uses a symmetric key and location key management, to achieve high en-routing filtering.

E.Limitation of Existing System

In Statistical En-route Filtering(SEF), the filtering probability at each sensor node is relatively low. It detects maximum of injected false reports. But does not consider the possibility of en-routing sensor nodes compromise. In Interleaved hop-by-hop authentication(IHA), if creation of association fails, it is vulnerable to attack. IHA uses the symmetric key for authentication, which allows the compromised nodes to misuse it to generate false reports. In location-Based Resilient Secrecy(LBRS) and Location-aware end-to-end security design(LEDS)requires extra overhead to achieve en-routing filtering. In LEDs all the nodes can determine their locations and generate location based keys which takes time.

III. PROPOSED SYSTEM

The design goal of proposed system is to achieve bandwidth efficient authentication for filtering injected false data. Every sensor node in wireless sensor network shares a private key with sink. Each node knows it'sone hop neighbor and establishes a public private key pair with each of them. In this scheme it use Message Authentication Code(MAC)mechanism to authenticate broadcast messages and every node can verify the broadcast messages. Each MAC is set to 1 bit to achieve bandwidth efficient authentication. To filter data injected by attacked sensor nodes. The proposed scheme adopts Cooperative Neighbor Router(CNR)based filtering mechanism asshown in figure1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014

International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

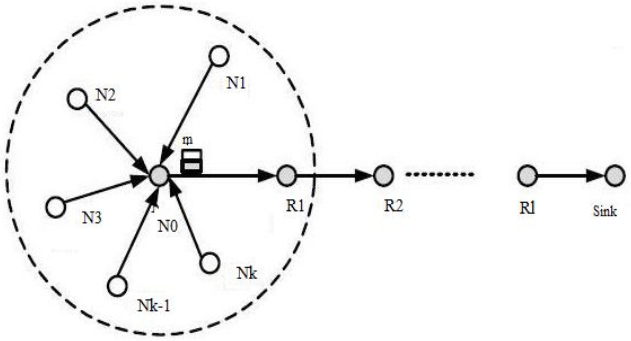

Fig-1.CNR Based Authentication Mechanism

Here a source node N0 is ready to send a report m to the sink via an established routing path PN0:{R1,R2…Rl, Sink}it first resorts to its kneighboring sensor nodes NN0:{N1,N2,…Nk} to cooperatively authenticate the report m, and then send it together with the authentication information MAC from N0 to sink via routing path RN0,where the sink initializes all sensor nodes, then each one of its shares its private key with sink. With this mechanism probability of k neighbors can be calculated, which also provides the necessary condition needed for authentication. With the proposed mechanism injected false data can be early detected and filtered. In addition the accompanied authentication information is bandwidth efficient.

IV. IMPLEMENTATIONMODULES

The following section depicts several practical design and implementation modules in building the proposed mechanism.

A. Sensor node initialization and deployment

The base station (sink), forwarding node, sensor nodes have been designed. The sink deploys these initialized sensor nodes at a Certain Interest Region(CIR).It is assumed that all sensor nodes are uniformly distributed in CIR after deployment. Sink initializes sensor nodes with unique ID. Sensor node chooses a private key from key pool and share with sink.

B. Routing establishment

In the proposed model,base station, forwarding node and sensor nodes have 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 base station. For this, sensor node and forwarding nodes must establish their neighbor nodes automatically, they establish a route to sink using the shortest path based on some existing routing protocol.

C. Sensed Results Reporting Protocol

To filter the false data injected by compromised sensor nodes, the proposed scheme adopts Cooperative Neighbor Router(CNR) based filtering mechanism. In the CNR based mechanism, when a sensor (source)node N0 has sensed some data m and is ready to report m to the sink via routing path RN0:{R1, R2,…R1,Sink}. The source node N0 gains the current time stamp T, chooses k neighboring nodes NN0:{N1,N2…Nk} and sends the report m. The source node N0 use key pair establishment to compute shared keys with each node in {N0, N1,N2…Nk}as{K1,K2…Kl,Ks}if Ni believes the report m is true then add MAC information with report send to sink along routing path.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014

International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

D. Filtering false injection attack

When each sensor node Ri, along the routing RN0 receives message m, timestamp T, and MAC from its upstream node, it checks the integrity of the message m and the timestamp T. If the timestamp T is out of date, the received message m, timestamp T and MAC will be discarded.

E. Sink Verification

Sink receives report m, Timestamp and MAC. Check the time, if the timestamp is unmatched or old, then the report will be discarded.

V. EXPERIMENTAL RESULTS

Filtering the false injected data is the main problem in wireless sensor networks. The proposed scheme is used to filter the injected false data by verifying the MAC of every node.

In proposed model sink, cluster head, and sensor node have been designed, sink 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 sink.

When each sensor node receives message m, timestamp T and MAC, it checks the integrity of message m, timestamp T, if timestamp T is out of date, the received message m, timestamp T and MAC will be discarded.

VI. CONCLUSION

Proposed Detection and Elimination of False Data in Wireless Sensor Network for Efficient Utilization of Bandwidth scheme for filtering the injected false data, has been demonstrated to achieve not only high en-routing filtering probability but also high reliability. Due to this the proposed scheme could be applied to other fast and distributed network where the authentication purpose is also distributed, e.g., authentication function in the wireless mesh network. It also adopts the bit compressed authentication technique to save bandwidth. Therefore, it is very suitable for filtering false data in wireless sensor networks and hence compromise-tolerant.

REFERENCES

[1] X. Lin, R Lu and Shen MDPA: Multidimensional Privacy-Preserving Aggregation Scheme for Wireless Sensor Networks, Wireless Comm. And Mobile Computing,2010.
[2] X. Lin, CAT: Building Couples to Early Detecting Node Compromise Attack in Wireless Sensor Network, IEEE GLOBECOM 2009.
[3] V.C. Giruka, M. Singhal, J .Royalty, and S.Varanasi, Security in Wireless Sensor Network, Wireless Comm and Mobile Computing, Jan 2008
[4] K Ren, W.Lou, Y.Zhang, Multi-User Broadcast Authentication in Wireless Sensor Networks, IEEE Sensor Ad Hoc Comm Networks 9SECON 07),June 2007.
[5] L Eschenauer and V D Gigor A Key Management Scheme for Distributed Sensor Networks, proc ninth ACM Conf,Computer and Comm Security(CCS 02),2002.
[6] A. Liu and P .Ning TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks ,proc.s eventh int'l conf. information Processing in Sensor Networks

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014

International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India