ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

AN EFFECTIVE SOURCE ROUTING FOR FALSE DATA INJECTION ATTACK IN WIRELESS SENSOR NETWORK

Madhuri N. Burange*, Prof. Venkat K. Jadhav

*1Student(M.E.), Department of EXTC, Navi Mumbai, Maharashtra, India

*2Assistant Professor, Department of Elex, Mumbai University, Maharashtra, India

ABSTRACT

Wireless sensor network (WSN) is an emerging technology that has resulted in a variety of applications. By using bandwidth-efficient cooperative authentication Network (BECAN) the false data injection filtering done efficiently and with less energy consumption . In WSN Sensor nodes are usually vulnerable to physical attacks or sensor node compromises easily. As the Sensor node could be easily compromised, the attacker can gain control obtain key values and change the properties of the node. This results in an false report to sink node and energy wastage in en-route nodes. In BECAN scheme the flase data injection and filtering done on the earlier stage which avoids false data injection, avoide unnecessary energy consumption in less time and with effieiency. Energy consumption avoid by checking only a very small amount of injected false data by the sink, it reduces the work load of the sink. The heart of BECAN scheme is cooperative neighbor router (CNR)-based filtering mechanism and it provides High Filtering Probability as well as high reliability

KEYWORDS: BECAN, Filtering Injecting, Wireless Sensor Networks, En-routed Nodes, Sink.

INTRODUCTION

In wireless sensor networking the research advances in nearby time as applications in modern life increases. A wireless sensor network is usually composed of a large number of sensor nodes interconnected through wireless links to perform sense the event or parameters. Each sensor node consist of necessary data sensing, processing, and communicating components. Hence, when a sensor node generates a report on an special event, e.g., a temperature change at surronding,will send a report to the data collection , sink through an established routing path. A sensor network must not only report each significant result promptly, but also reject false reports injected by attackers. Various security attacks. are very vulnerable in Wireless sensor networks The most serious and dangerous one is suffering from injecting false data attack .

For this injected false data attack, first several sensor node are compromised by an attacker .When any sensor node is compromised then the attacker accesses all keying materials stored in the compromised nodes process it and send the false data to the sink . Due to this false event is triggered and the false report send to the sink.

Various adverse effects of this attack are large no of expensive resources wastage,Energy wastage, heavy verification burdens on the sink. It could paralyze the entire network quickly. Therefore, to mitigate the energy waste, the filtering of false data should be carried out as early as possible. It is difficult to find a node once compromised while most of these filtering mechanisms use the symmetric key technique. It can be described that the compromised node abuses its keys to generate false reports and reliability of the filtering mechanisms degrade

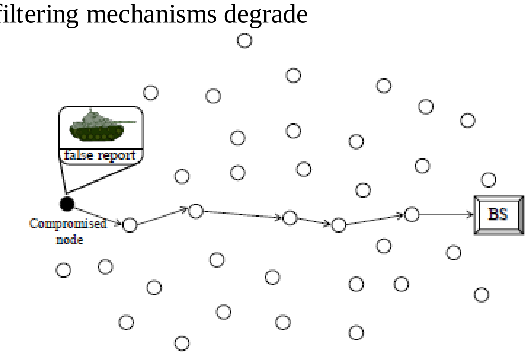

Figure1:Wireless sensor network

Where as the proposed mechanism BECAN resolves this problem. In this early detecting and filtering the majority of injected false data take place hence can save energy. The sink needs to verify a very small fraction of injected false data, thus largely reduces the burden of the sink. Its clear that compared with the previous mechanisms, this new mechanism achives maximum filtering probability and high reliability.

MODE AND DESIGN GOAL

Network Model

We consider a typical wireless sensor network which consists of a sink and a large number of sensor nodes N = {N0, N1, . . .} randomly deployed at a certain interest region (CIR) with the area S. The sink is a trustable and powerful data collection device, which has sufficient computation and storage capabilities and is responsible for initializing the sensor nodes and collecting the data sensed by these nodes. Each sensor node Ni € N is stationary in a location. For differentiation purpose, we assume each sensor node has a unique nonzero identifier. The communication is bidirectional, i.e., two sensor nodes within their wireless transmission range (R) may communicate with each other. Therefore, if a sensor node is close to the sink, it can directly contact the sink. However, if a sensor node is far from the transmission range of the sink, it should resort to other nodes to establish a route and then communicate with the sink.

Security Model

Since a wireless sensor network is unattended, a malicious adversary may readily launch some security attacks to degrade the network functionalities. In addition, due to the low-cost constraints, sensor nodes N={N0,N1, . . .} are not equipped with expensive tamper-proof device and could be easily compromised in such an unprotected wireless sensor network.

In our security model the position of the sensor node is stored during the initialization phase the adversary cannot launch compromise node attack, where a group of nodes are controlled and moved by the adversary. The position information also greatly reduces reaffiliations per unit time. The report embedded with timestamp T resist replay attack. The energy consumption also reduces with short route paths, this implies scalability of BECAN scheme.

Design Goal

The design goal is to develop an efficient cooperative bandwidth-efficient authentication scheme for filtering the injected false data. The two desirable objectives are as follows.

1.Early Detecting the Injected False Data by the EnRoute Sensor Nodes

The sink is said to be trustable and powerful data collection device. Undoubtedly, the sink will become a bottleneck if authentication is done at sink. If the entire authentication task is fulfilled by the sink, this greatly increases the burden of the sink and can bottleneck the sink. The authentication by en-route sensor node helps in early detection of injected false data and thus can save energy adding a minor overhead at the en-route sensor node.

2.Achieving Bandwidth-Efficient Authentication

A bandwidth efficient authentication method has to be designed because costs of sensor node are low and energy constraintA Message Authentication Code (MAC) is produced so as to authenticate the transmitted data through the en-route nodes. MAC is one bit, thus making bit-compressed authentication possible.

PRAPOSED BECAN SCHEME

To filter the false data injected by compromised sensor nodes, the BECAN adopts cooperative neighbor _ router(CNR)-based filtering mechanism. In the CNR-based mechanism, when a source node N0 is ready to send a report m to the sink via an established routing path RN0 : [R1-> R2 ->Rl -> Sink], it first resorts to its k neighboring nodes Nn0 : {N1,N2, . . .Nk} to cooperatively authenticate the report m, and then sends the report m and the authentication information MAC from N0 ỤNn0 to the sink via routing Rn0.

METHODOLOGY

The framework for the proposed scheme for CBA authentication is shown in below Figure.

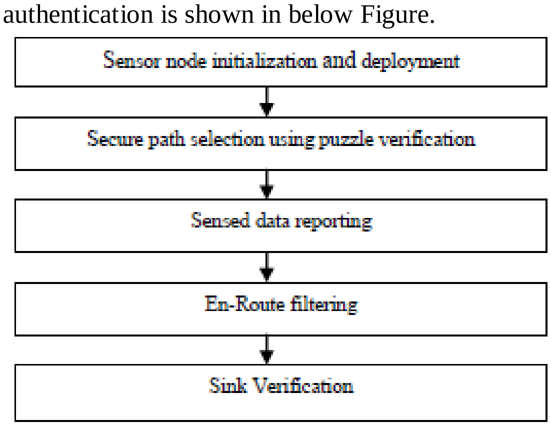

Figure 2 : Steps in CBA Authentication

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

DESCRIPTION OF BECAN AUTHENTICATION

The BECAN authentication scheme consists of two phases: sensor nodes initialization and deployment, and sensed results reporting protocol.

A Cooperative Bit-Compressed Authentication (CBA) scheme for filtering injected false data in Wireless Sensor Networks (WSN) has been proposed. The two main phases are:

A. Safe path selection.

B. Authentication and verification of sensed data.

A .Sensor Nodes Initialization and Deployment:

Given the security parameter k, the sink first chooses an elliptic curve defined over , where p is a large prime and G is a base point of prime order q with . Then, the sink selects a secure cryptographic hash function , where . Finally, the sink sets the public parameters as params. To initialize sensor nodes N={n1,n2,n3…..} the sink invokes the

Algorithm 1. Then, the sink deploys these initialized sensor nodes at a CIR in various ways, such as by air or by land. Given the rich literature in wireless sensor node deployment we do not address the deployment in detail. Without loss of generality, we assume that all sensor nodes are uniformly distributed in CIR after deployment.

All sensor node are uniformly and randomly deployed at CIR.

When the sensor nodes are not involved in reporting task, they cooperatively establish shortest path, by AODV existing routing protocol. This can accelerate reporting of sensed data.

STEP1 : Choose the number of sensor nodes.

STEP2 : Store the location of each sensor node.

STEP3 : Preload each sensor node with public key.

STEP4 : Choose the shortest path using 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

B. Sensed Result Reporting Protocol

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.

The report m generated by sensor node by sensing of any parameters are send to the sink via, established shortest and safest path selected.

Assume that, the sensor (source) node N0 has sensed some data m and is ready to report m to the sink via the routing path RN0:[R1->R2- >……Rn->sink].

, the following protocol steps will be executed:

Step 1. The source node N0 gains the current time stamp T, chooses k neighboring nodes Nn0:{N1N2…Nk} and sends the event (m,T) and routing Rn0 to Nn0 .

Step 2. With(mT,Rn0)as input, each sensor node Ni €(Nn0Ụ{n0}) invokes the Algorithm 2 to generate a row authentication vector and reports rowi,to the source node N0.

C. En-Routing Filtering

When each sensor node R_i, $(1 \leq i \leq l)$, along the routing RN0 receives (m, T, 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 message (m, T, MAC) will be discarded. If the returned value is "accept," R_i will forward the message (m, T, MAC) to its downstream node, Otherwise, (m, T, MAC) will be discarded

STEP1 : Checks the timestamp T.

STEP2 : Each en-route sensor node uses noninteractive keypair establishment to compute shared keys with each sensor node.

STEP3 : If m is cooperatively authenticated by k neighbour nodes the report is MAC verified.

D. Sink Verification

If the sink receives the report (m, T, MAC), it checks the integrity of the message m and the timestamp T. If the timestamp is out of date, the report (m, T, MAC) will be immediately discarded. Otherwise, the sink looks up all private keys k_{is} of N_i, $0 \leq i \leq k$.

Sink on receiving the report checks the integrity of *R* and timestamp T. If T is outdated *R* is rejected otherwise *R* undergoes sink verification.

STEP1 : Checks the timestamp T.

STEP2 : Sink looks up all private keys $k_{is.}$

E. Reliability of BECAN Scheme

. In addition to the high (en-routing) filtering probability, the BECAN scheme also has high reliability, i.e., even though some sensor nodes are compromised, the true event reports still can reach the sink with high probability.

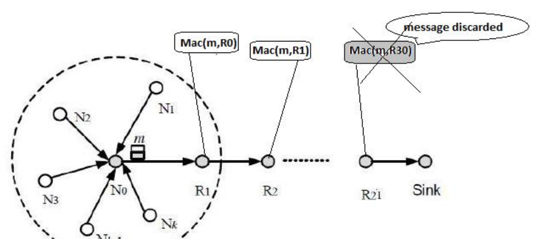

Figure 3 : Co-operative CNR based Authentication

PERFORMANCE EVALUATION

The performance of the BECAN scheme depends on the following characterstics.

False Negative Rate (FNR).

FNR= Number of true data that cannot reach the sink/Total number of true data

If FNR is small then the high reliability.

En-Route Filtering Probability (FPR).

FPR= Number of false data filtered at en-route nodes /Total number of false data

The en-routing filtering probability FPR in terms of different number of en-routing nodes. As the number of routing nodes increases, FPR increases.

Reaffiliations per unit time.

Reaffiliations per unit time implies the redundancy of transmitted data.

Throughput.

Throughput= Number of packet received /Time

Energy consumption.

The majority of injected false data can be filtered by BECAN scheme within short number of hops during transmission. Thus, it can greatly save the energy of sensor nodes along the routing path.

CONCLUSION

A CBA scheme for filtering injected false data and preventing compromise node attacks had been analyzed. By theoretical analysis . The BECAN scheme has been demonstrated to achieve not only high en-routing filtering probability but also high scalability. Due to the ease and efficiency, the BECAN scheme could be applied to other fast and distributed authentication scenarios

.

REFERENCES

1. Rongxing Lu. and Xiaodong Lin., “BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks,” IEEE transactions on parallel and distributed systems, vol. 23, no. 1, Jan. 2012.
2. Teenu Liza Thomas and P. Vijayalakshmi “ Cooperative Bit-Compressed Authentication Scheme against Compromised Node Attacks in Wireless Sensor Networks” *International Journal of Computer Applications (0975 – 8887) Volume 71– No.19, June 2013*
3. Nithya Menon, S.Praveena” BECAN: A Bandwidth Efficient Cooperative Authentication Scheme for Wireless SensorNetworks” **International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-6, May 2013**
4. 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.
5. 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.
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.