Filtering False Data in the Networks

Mr. Mohammed Danish
Asst Professor,
Dept of Computer Application GIMS,
Bangalore

***Abstract*--.Injecting false data attack is a well known serious threat to wireless sensor network, for which an adversary (enemy) reports bogus information to sink (data collection unit) causing error and energy waste in en-route nodes. Here this project proposes a false data filtering scheme for filtering injected false data in networks. Based on the random graph characteristics of sensor node deployment and the cooperative bit compressed authentication technique, this scheme can save energy by early detecting and filtering the majority of injected false data. In addition, the sink must only verify the injected data, which thus largely reduces the burden of the sink. Thus, this scheme provides high filtering probability and is energy saving.**

I INTRODUCTION

It has been well recognized for some emerging applications, such as tracking for military troops. A wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. Each Sensor node is low-cost but equipped with necessary sensing, data processing, and communicating components. Therefore, when a sensor node generates a report after being triggered by a special event, e.g., a surrounding temperature change, it will send the report to a data collection unit (also Known as sink) through an established routing path .Wireless sensor networks are usually deployed at unattended environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes, and Sybil attacks. In addition, wireless sensor networks may also suffer from Injecting false data attack. For an injecting false data attack, an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes, and then controls these compromised nodes to inject bogus information and send the false data to the Sink to cause error decision, as well as energy wasted in en-route nodes. For instance, an adversary could fabricate a wildfire event or report a wrong wildfire location information to the sink, then expensive resources will be wasted by sending rescue workers to a non existing or Wrong wildfire location. Therefore, it is crucial to filter the false data as accurately as possible in wireless sensor networks. At the same time, if all false data are flooding into the sink simultaneously, then not only huge energy will be wasted in the en-route nodes, but also heavy verification burdens will undoubtedly fall on the sink. As a result, the whole network could be paralyzed quickly. Therefore, filtering false data should also be executed as early as possible to mitigate the energy waste. To tackle this challenging issue, some false data filtering mechanisms have been developed. Since most of these filtering mechanisms use the symmetric key technique, once a node is compromised, it is hard to identify the node. In other words, the compromised node can abuse its keys to generate false reports, and the reliability of the filtering mechanisms will be degraded. This project is a course of action, in which the amount of data that is to be transmitted through the nodes under privacy of individual user with minimum waste of energy. Compared with the previously reported mechanisms, this scheme achieves not only high filtering probability but also high reliability. First, we study the random graph characteristics of wireless sensor node deployment, and estimate the probability of k-neighbors, which provides the necessary condition for false data filtering authentication. Second, we propose this scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data can be early detected and filtered by the en-route sensor nodes.

2 MODELS AND DESIGN GOAL

Here, we formulate the network model, the security model, and identify the design goal.

2.1 Network Model

We consider a typical wireless sensor network which consists of a sink and a large number of sensor nodes 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 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. .

2.2 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 are not equipped with expensive tamper-proof device and could be easily compromised in such an unprotected wireless sensor network. Therefore, in our security model, we assume an adversary can compromise a fraction of sensor nodes and Then, after being controlled and reprogrammed by the adversary, these compromised sensor nodes can collude to launch some injected false data attacks. Since our work focuses on filtering injected false data attack, other attacks launched by the compromised sensor nodes in wireless sensor network, such as building bogus routing information, selectively dropping true data packet, and creating routing loops to waste the energy of network, are not addressed in this project.

2.3 Design Goal

The design goal is to develop an efficient cooperative bandwidth-efficient authentication scheme for filtering the injected false data. Specifically, the following two desirable objectives will be achieved.

2.3.1 Early Detecting the Injected False Data by the En-Route Sensor Nodes

The sink is a powerful data collection device. Nevertheless, if all authentication tasks are fulfilled at the sink, it is undoubted that the sink becomes a bottleneck. At the same time, if too much injected false data floods into the sink, the sink will surely suffer from the Denial of Service (DoS) attack. Therefore, it is critical to share the authentication tasks with the en-route sensor nodes such that the injected false data can be detected and discarded early. The earlier the injected false data is detected, the more energy can be saved in the whole network.

2.3.2 Achieving Bandwidth-Efficient Authentication

Since the sensor nodes are low-cost and energy constraint, it is desirable to design a bandwidth efficient authentication scheme.

3 PRELIMINARIES

3.1 Tiny ECC-Based Non interactive Key pair Establishment

Tiny ECC is a configurable library for Elliptic Curve Cryptography (ECC), which allows flexible integration of ECC-based public key cryptography in sensor network applications. Ready-to-use Tiny ECC is suitable for wireless sensor networks to provide convenient authentications and pair key establishments. In other words, if a sensor node is compromised, then the key shared between two nodes will be disclosed. However, the key shared between other sensor nodes is not affected.

3.2 Message Authentication Code in ZZ2n

Message authentication code (MAC) provides assurance to the recipient of the message which came from the expected sender and has not been altered in transit [24].

4 PROPOSED FDFN SCHEME

In this section, we will propose FDFN scheme for filtering injected false data in wireless sensor networks. Before preceding the scheme, the design rationale is introduced.

4.1 Design Rationale

To filter the false data injected by compromised sensor nodes, the FDFN adopts cooperative neighbor **_** router (CNR)-based filtering mechanism. As shown in Fig. 3, in the
DIAG IS THERE

4.2 Description of FDFN Authentication

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

4.2.1 Sensor Nodes Initialization and Deployment

Given the security parameter _, the sink first chooses an elliptic curve cryptograph to initialize the sensor node. the sink invokes the Algorithm . Then, the sink deploys these initialized sensor nodes at a CIR in various ways, such as by air or by land. we assume that all sensor nodes are uniformly distributed in CIR after deployment.. Once an event occurs, a report can be immediately relayed along the established routing path.

Algorithm1: SENSORNODESINITIALIZATION

```
procedure sensor node initialization
   Input: prams and un-initialized nodes N
  Output: initialized nodes N0
for each sensor N0 belongs to N do
preload N0 with Tiny ECC, prams and energy
choose a random number public key x,
Compute the private key y=X*G and install (Y, X) in node
end for
return initialized node N
end procedure
```

4.2.2 Sensed Results 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. 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 to the sink. Sink, as shown in Fig.3

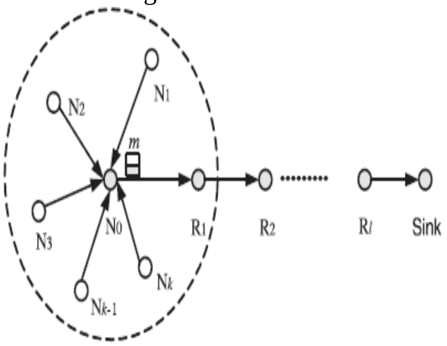

Fig. 3. Cooperative CNR-based authentication mechanism.

The following protocol steps will be executed:

Step 1. The source node N0 gains the current timestamp T, chooses k neighboring nodes, and sends the event to the node.

Step 2. With message as input, each sensor node invokes the Algorithm 2 to generate a row authentication vector and reports Row to the source node N0.

Algorithm2: CNRBASEDMACGENERATION

```
procedure: CNRBASEDMACGENERATION
    Input: prams, NO belongs to N , M,T,R
    Output: row
NO uses non-interactive key pair establishment to compute shared keys with each node N0 :[N1,N2,………Nn ….sink] K1, K2, …..K1S, where k1s is N0'S private key distributed by the sink
if N0 believes the report M is true then a neighboring node is assumed having same ability to detect a true event as source node & correctly judge the report M.
    for j=1 to l do
        MACij = MAC (M||T, Kij , 1)
    end for
    MACis = MAC (M||T, Kis, a)
else
    for J=1 TO l do
        MACij is set random bit
    end for
    MACis is set as a random bit string of length a
end if
return Row= ( MACi1, MACi2…MACis)
end procedure
```

Step 3. After the source node N0 aggregates all row vectors it formats the authentication information MAC as

$$\mathrm{MAC} = \begin{pmatrix} Row_0 \\ Row_1 \\ Row_2 \\ \vdots \\ Row_k \end{pmatrix} = \begin{pmatrix} mac_{01} & \cdots & mac_{0l} & mac_{0s} \\ mac_{11} & \cdots & mac_{1l} & mac_{1s} \\ mac_{21} & \cdots & mac_{2l} & mac_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ mac_{k1} & \cdots & mac_{kl} & mac_{ks} \end{pmatrix},$$

and reports (M,T,MAC) to the sink along the routing .

4.2.3 En-Routing Filtering

When each sensor node, along the routing receives message; 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 will be discarded. Otherwise, invokes the Algorithm 3. If the returned value is "accept will forward the message m to its downstream node.

Algorithm3: 3CNRBASEDMACVERIFICATION

```
procedure CNR based MAC verification
    Input: prams, M, T, N
    Output: ACCEPT or REJECT
node uses non-interactive key pair establishment to compute shared key as with each node a key.
set return value = "accept"
for I=0 to k do
    $\underline{MACij}$ = MAC(M||T, Kij, 1)
    if $\underline{MACij}$ + MACij not equal to 0 then
        set return value = "reject"
        break
    end if
end for
return return value
end procedure
```

4.2.4 Sink Verification

If the sink receives the report m;, it checks the integrity of the message m and the timestamp T. If the timestamp is out of date, the report m will be immediately discarded. Otherwise, the sink looks up all private keys and invokes the Algorithm 4.

If the returned value of Algorithm 4 is "accept," the sink accepts the report m; otherwise, the sink rejects the report.

Algorithm 4: Sink Verification

```
procedure SINKVERIFICATION
    Input: prams,K1s, K2s…(M, T, N)
    Output: ACCEPT or REJECT
set return value = "accept"
for I=0 to k do
    $\underline{MACij}$ = MAC(M||T, Kij, 1)
    if $\underline{MACij}$ + MACij not equal to 0 then
        set return value = "reject"
        break
    end if
end for
return return value
end procedure
```

5 SECURITY ANALYSES

In this section, we analyze the security of the FFDN authentication scheme with respect to our main design goal, i.e., the effectiveness of filtering the injected false data.

5.3 Discussion on Gang Injecting False Data Attack

In this section, we introduce a new stronger injecting false data attack, called gang injecting false data attack, in wireless sensor networks. This kind of attack is usually Launched by a gang of compromised sensor nodes controlled and moved by an adversary A. false data, several compromised nodes will first move and aggregate at the source node, and then collude to inject the false data. Because of the mobility, the gang injecting false data attack is more challenging and hard to resist. To tackle this kind of attack, a possible solution with the FFDN scheme is to require each participating sensor node to provide its position information. If the current position is not consistent with the previous ones, the gang attack can be detected. Nevertheless, how to prevent/mitigate the gang injecting false data attack from mobile compromised sensor nodes is still worthy of the further investigation.

6 PERFORMANCE EVALUATIONS

Energy saving is always crucial for the lifetime of wireless sensor networks. In this section, the performance of the proposed FFDN scheme is evaluated in terms of energy efficiency.

6.2 Energy Consumption in Transmission

The majority of injected false data can be filtered by FFDN during transmission. Thus, FFDN can greatly save the energy of sensor nodes along the routing path.

7 RELATED WORK

Recently, some research works on bandwidth-efficient filtering of injected false data in wireless sensor networks have been appeared in the literature in. Tung you Ye et al. propose a statistical en-routing filtering mechanism called SEF. SEF requires that each sensing report. To avoid putting all eggs in one basket, FFDN distributes the en-routing authentication to all sensor nodes along the routing path. To save the bandwidth, it also adopts the bit-compressed authentication

Technique. Therefore, it is compromise-tolerant and suitable for filtering false data in wireless sensor networks.

8 CONCLUSION

In this project, we have proposed a FFDN scheme for filtering the injected false data, the FFDN scheme has been demonstrated to achieve not only high en-routing filtering probability but also high reliability. Due to the simplicity and effectiveness, the FDFN scheme could be applied to other fast and distributed authentication scenarios, e.g., the efficient authentication in wireless mesh network.

9 FUTURE WORK,

we will investigate how to prevent/mitigate the gang injecting false data attack from mobile compromised sensor nodes [32].

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. (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.

[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks,” Proc. IEEE Symp. Security and Privacy, 2004.