False Data Filtration in Wireless Sensor Networks using Bloom Filter

S.Dhivyabharathi¹, S.Baskaran²,

¹Student, Sri Manakula Vinayagar Engineering College, Pondicherry, ²Assistant Professor, Sri Manakula Vinayagar Engineering College, Pondicherry,

ABSTRACT

Injecting false data attack is a well known serious threat to wireless sensor network, for which an adversary reports false information to sink thereby causing error decision at upper level. If undetected this false reports would be forwarded to the data collection point. Such attacks by compromised nodes can result in not only false alarms but also the depletion of the finite amount of energy in the battery powered network. In this work, we propose a scheme for filtering the injected false data based on Bloom filter which is called modified Bandwidth Efficient Cooperative Authentication (BECAN) scheme. This modified BECAN scheme can save energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route node. In addition, only a very small fraction of injected false data needs to be checked by the sink, which thus largely reduces the burden of the sink. The simulation results are given to demonstrate the effectiveness of the proposed scheme in terms of high filtering probability and energy saving.

Key words: False data, Compromised nodes, BECAN, Bloom filter.

I INTRODUCTION

A wireless sensor network is composed of a large number of sensor nodes interconnected through wireless links. The primitive objective of WSNs is to answer queries by gathering sensory data from the deployed sensors. The process of collecting sensory data is generally called as ‘aggregation’. Since sensor nodes in WSN technology are usually tiny micro-electronic devices which have limited resources like low processor speed, small memory size, low computation and communication power, it becomes very challenging to design mechanisms which support data queries.

Basically, a wireless sensor network consists of a number of tiny sensor nodes connected together through wireless links. Some more powerful nodes may operate as control nodes called base stations. Often, the sensing nodes are referred to as ‘motes’ while base stations are sometimes called as ‘sinks’. Each sensor node can sense data such as temperature, humidity, pressure from its surroundings, conduct simple computations on the collected data and send it to other neighbouring nodes through the communication links. Control nodes may further process the data and transfer it to a database server via a wired communication.

Wireless sensor networks are usually deployed at unattended or hostile environments. Therefore they are 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. To inject false data, an adversary first compromises sensor nodes, accesses all keying materials stored in the compromised node and then controls these compromised nodes to inject false data to the sink to cause upper-level error decision, as well
as energy wasted in en-route nodes. Therefore false data should be early detected and filtered to mitigate the energy waste.

In this paper, we propose a modified Bandwidth Efficient Cooperative Authentication (BECAN) scheme to filter the injected false data in wireless sensor networks in an early stage based on bloom filter. First we provide a non-interactive key pair establishment among all nodes using RSA. Then every node generates a message authentication code using message digest5 hashing algorithm. When a source node is ready to send the data, it first gets authentication cooperatively from its neighbouring nodes and then forwards. The data which is forwarded is compressed using bloom filter. Each en-route route checks for the data integrity based on the received bloom filter.

II RELATED WORK

The sender wants to send data as soon as possible in a secured manner in any network. One of the major issue in wireless sensor networks is the limited battery, attackers take this into account and inject false data thus consuming higher energy by each forwarding nodes.

An efficient secure data aggregation is proposed by Priyanka S. Fulare, Nikita Chavhan [1] to enhance the data security of wireless sensor networks. The reduction in overall energy consumption for a real-time data acquisition system is addressed by C.Bennila Thangammal, P.Rangarajan, J.Raja Paul Perinban [2].

A comparative study on the various symmetric keying technique is proposed by Monika Agrawal, Pradeep Mishra [3] to conserve energy in keying techniques. The problem of early detecting the false data is addressed by Rongxing Lu et al. [4], in novel bandwidth efficient cooperative authentication (BECAN) scheme for filtering the injected false data.

Zhen Yu and Yong Guan [5], uses Dynamic en-route filtering scheme to filter injected false data and DoS attack in wireless sensor networks. Each node uses its own auth-keys to authenticate their reports. The auth-keys of each node form a hash chain are updated in each round. The cluster-head disseminates the first auth-key of every node to forwarding nodes and then sends the reports followed by disclosed auth-keys. The forwarding nodes verify the authenticity of the disclosed keys by hashing the disseminated keys and then check the integrity. According to the verification results, they inform the next-hop nodes to either drop or keep on forwarding the reports. This process is repeated by each forwarding node at every hop.

Data Reporting in Wireless Sensor Networks Using Dynamic Filtering Scheme is proposed by Sachin S Hiremath, D. Geetha and Harshapriya Chatnalkar [6]. A Statistical En-Route Filtering of Injected False Data in sensor networks is proposed by Fan Ye, Haiyun Luo, Songwu Lu [7]. This scheme divides the global key pool into multiple partitions and then assigns a certain number of keys to individual nodes. Thus any single node does not know the entire information of the network which makes difficult for the intruders to compromise.

The design, implementation, and evaluation of Tiny ECC, a configurable library for ECC operations in wireless sensor networks is proposed by A. Liu and P. Ning [8].
Y. Zhang, W. Liu, W. Lou, and Y. Fang [9], proposed a Location-based compromise-tolerant security mechanism for wireless sensor networks. Node compromise is a serious threat to wireless sensor networks deployed in unattended and hostile environments. To mitigate the impact of compromised nodes, they propose a suite of location-based compromise tolerant security mechanisms.

III PROPOSED WORK

The steps in the proposed scheme is discussed below:

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). The sink is a trustable and powerful data collection device, which has sufficient computation and storage and is responsible for initializing the sensor nodes and collecting the data sensed by these nodes.

A) Non-interactive key pair establishment

For any two sensor nodes, no matter whether it is within the transmission range or not, a key pair can be established between them without direct contact. The key generation is based on RSA algorithm. The established keys are independent. Each key pair consists of a private and a public key.

\[ k = x \times y \]

where,

x- private key
y- public key

Once the key is generated, the message which is to be sent is encrypted using RSA encryption technique. The encrypted message and the key is used to generate message authentication code.

B) Message Authentication Code

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. Let h(.) be a secure cryptographic hash function.

\[ MAC = h( m , k ) \]

Where, m and k are message and key. The hashing function used is message digest 5 (MD5), since the input to this hashing algorithm can be infinite and produces an output of 128 bits.

C) Cooperative Authentication

To filter the false data injected by compromised sensor nodes, the modified BECAN scheme adopts cooperative neighbour x router (CNR) based filtering mechanism as shown in the Fig.1
In the CNR-based mechanism, when a source node is ready to send a report m to the sink via an established routing path, it first resorts to its k neighbouring nodes to cooperatively authenticate the report m, and then sends the report m and the authentication information MAC from N0 ∪ N_{N0} to the sink via routing R_{N0}.

\[
\text{MAC} = \begin{pmatrix}
\text{mac}_0 & \ldots & \text{mac}_0l & \text{mac}_0s \\
\text{mac}_1 & \ldots & \text{mac}_1l & \text{mac}_1s \\
\vdots & \ddots & \vdots & \vdots \\
\text{mac}_k & \ldots & \text{mac}_kl & \text{mac}_ks
\end{pmatrix}
\]

D) Bloom Filter

A Bloom filter is a space efficient data structure that is used to test whether an element is a member of a set. Bloom filters require constant time to add an element to the set or test for membership, regardless of the size of the elements or the number of elements already in the set. No other data structure has this property.

The MAC which is generated is not sent as such, instead it is compressed using hashing and a bloom filter array is formed. Thus the scheme is bandwidth efficient since the data is compressed and sent.

A bloom filter is formed by following steps:

Step 1: An m-bit array is formed with all bits 0

| 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 |

Step 2: Each item(X_i) in the set MAC is hashed k times, with each hash yielding a bit location and these bits are set to 1
Step 3: To check if an element $y$ is in the set, hash it $k$ times and map it to the corresponding bits

If all the bits are 1 then the message is forwarded to the next hop, else the message is dropped.

IV SIMULATION SETTINGS

A network simulator 2 is used to study the comparison of BECAN scheme and mBECAN (modified BECAN) in terms of filtering probability and filtering ratio.

In the simulation 100 sensor nodes with a transmission range of 50 m are randomly deployed in an area of $600 \times 600$ m$^2$. The number of hops between the source node and the sink node is considered to be 10. The routing protocol used in our simulation is AODV (Ad hoc On Demand Distance Vector). AODV is chosen as routing protocol since it does not require any central administrative system to control the routing process and reacts relatively fast to the topology changes in the system. The parameters used in the simulation is shown in the below table 1.

Table 1. Simulation Parameters

<table>
<thead>
<tr>
<th>PARAMETERS</th>
<th>VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation area</td>
<td>$600m \times 600m$</td>
</tr>
<tr>
<td>Transmission range</td>
<td>50m</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>50</td>
</tr>
<tr>
<td>Number of hops</td>
<td>10</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Simulation time</td>
<td>100s</td>
</tr>
</tbody>
</table>
V PERFORMANCE ANALYSIS

Fig 2. shows the en-routing filtering probability in terms of different number of en-routing nodes. The filtering probability is the ratio of the number of false data filtered by the en-route nodes to the total number of false data injected.

\[
\text{Filtering probability} = \frac{\text{Number of false data filtered by en-route nodes}}{\text{Total number of false data}}
\]

As the number of routing nodes increases, filtering probability also increases. It is evident from the graph that the modified Bandwidth Efficient Cooperative Authentication scheme achieves filtering probability of 0.8 whereas the BECAN scheme achieves 0.69.

Fig 3. shows the Filtering ratio at each en-routing node. The filtering ratio is defined as the ratio of the number of false data filtered at each node to the total number of false data entering the node.

\[
\text{Filtering ratio} = \frac{\text{Number of false data at each node}}{\text{Total number of false data entering the node}}
\]

From the graph it is evident that the filtering ratio of the modified BECAN scheme is 0.49 at first node whereas the in BECAN scheme it is 0.39. This proves that the modified Bandwidth Efficient Cooperative Authentication Scheme is more energy efficient as the false data is early detected and filtered.
Fig 3. Filtering Ratio

Fig 4. below shows the comparison of power consumption by each node in both BECAN and mBECAN scheme. The power consumed for generating key and providing authentication for message by each node in mBECAN scheme is approximately 62mW, whereas BECAN scheme consumes approximately 42mW, However, the overall power consumption is proved to be less in the proposed work.

Fig 4. Power consumption for key generation
Fig 5. below shows the overall power consumption at each node. From the graph, it is distinct that the power consumed by each node in mBECAN scheme is 132 mW and in BECAN scheme it is 163mW, proving that the mBECAN saves energy upto 30mW.

![Graph showing power consumption](image)

**Fig 5. Overall Power Consumption**

From the graph, it is seen that the power consumed by each node in modified BECAN scheme is less when compared to the BECAN scheme.

In wireless sensor network it is well known that the energy consumed in data transmission is greater than the energy consumed in data processing. Since the Bandwidth Efficient Cooperative Authentication Scheme allows some of the false data to travel through the en-route nodes, the power consumed by the intermediate nodes is high. This problem is been overcome by modified BECAN scheme as it detects and filters the false data in an early stage, the power consumption is less.

**VI CONCLUSION**

In this paper we proposed a modified Bandwidth Efficient Cooperative Authentication scheme. It detects and filters the injected false data based on bloom filter. It is observed from the result that the modified BECAN scheme achieves better en-routing filtering probability, filtering ratio and low power consumption. Since the data is been compressed and sent it is also bandwidth efficient. Energy saving is always an important issue for the lifetime of
wireless sensor networks. The result shows that the proposed system has great advantage in terms of energy consumption, security of data and also the communication cost.

VII REFERENCES


