Authenticated and Security Maintenance in Wireless Sensor Network by Filtering Injected False Data

L Devi1*, S P Shantharajah2 and A Nirmal Kumar3

1Bharathiar University, Coimbatore
2Sona College of Technology, Salem
3Department of IT, Veltech Hightech Dr RR Dr SR Engineering Colleg, Chennai

Received 23 May 2015; revised 22 February 2016; accepted 04 August 2016

A large sensor network with the individual sensor nodes focus to the security factor. A node injected into the sensor network for the data forwarding, causes some attacks. Such attacks lead to the injection of false data in the wireless sensor network. Wireless sensor networks are organized at aggressive backgrounds with most vulnerable attacks. In a large scale wireless sensor network, detecting reports injected by compromised nodes is a large research confront. Once a node is compromised, all the security information accumulates in that node turn out to be accessible to the attacker. In such sensor network, the improved authentication system is developed in research work to improve the security level by filtering the injected false data. The WSN focus on removing the injected false data attack and their mitigation technique is developed for high security maintenance. Perform the high security with the filtering of the injected false data should also be executed as early as possible.

Keywords: Wireless Sensor Network, NAEC, BO-GIDF, Resource Utilization, Watermarking.

Introduction

Collection of sensor nodes are the wireless sensor nodes that contains limited battery life, computational capabilities, storage and bandwidth. Multipath routing in WSN tolerate the failure of sensor nodes and improve the reliability of data routing. In addition, Resource utilization and security plays a significant role in WSN and many research works has been intended for multipath sensor network route path. The sensor nodes in WSN communicate with the physical world at an extensive level to provided advantages to several new applications. However, false data injection has posed significant challenges in wireless sensor network. A new framework named Localized Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) framework is designed to handle group injected false data. Network Authenticated based on ElGamal Cryptography (NAEC) framework is designed in WSN based on asymmetric key encryption. Implicit Authorized Certificate Rule is introduced to maintain high degree of interoperability. Resource Usage Control based Packet Data Watermarking mechanism efficiently controls the time of accessing the resources and resource utilization level. Finally, it broadcast the data packet without malicious adversaries on multipath route.

Aim and objective of this research

The aim of this research is to provide high authentication scheme without any false data injection. The proposed framework reduces the processing time in identifying the malicious adversaries. The objectives of this research are listed subsequently:

- To improve the bandwidth efficiency rate by applying Group based Neighbor Collaborative Selection model.
- To avoid the injection of false data, Implicit Authorized Certificate Rule is designed.
- To improve authentication scheme on sensor network by overcoming the false data injection, a framework called Network Authenticated based on ElGamal Cryptography (NAEC) is developed.
- To improve the security without any false data injection, Resource Usage Control based Packet Data Watermarking mechanism is introduced.
- To reduce the resource utilization in multipath sensor network route path. RUCPDW mechanism is proposed.

Proposed research methodology

The proposed research work focuses on improves network security by formulating a neighbor selection mechanism. Network Authenticated based on ElGamal Cryptography avoid the injection of false
data on dynamic paths. With this, the processing time is reduced in identifying the malicious adversaries. Watermarking procedure forward the packet data to the destination end with minimizing the energy consumption and therefore improves the security level. The proposed research work is carried out in different sources as shown in figure 1.

Localized bandwidth optimal group injected data filtering framework

The BO-GIDF framework is developed to group the sensor nodes based on the collaborative neighbor function and improve the bandwidth in an efficient manner. To improve packet transmission and network security, a Time-efficient Sink Detection algorithm is designed. Finally, an effective Associative Filtering scheme is applied to minimize the processing time for significant amount of packet transmission.

Group based Collaborative Neighbor Selection

Group based Collaborative Neighbor Selection mechanism is used to group injecting false attack from sensor nodes. It improves bandwidth efficiency by identifying whether the node is injected with false data or not in WSN. The mobile compromised node is obtained according to the movement of the sensor node from one position to another within the time routers. It is identified for sending the packet information to the sink node. Once the sink node obtains the information, the framework BO-GIDF checks the packet integrity with the help of the packet and the time of occurrence of event.

The occurrence of mobile compromised node is ‘MCN’ obtained if the sensor node is moved from one place ‘$S_{i+1}$’ to another ‘$S_{i+1,i+1}$’. As soon as an event is identified, then the information (i.e., packet) is transferred to the sink node ‘SN’ through organized routing efficient routers ‘$R_1, R_2, ..., R_n$’. With this, the source node (i.e., group node) ‘$S_1, S_2, ..., S_n$’ obtains the time of occurrence of event ‘$T$’, by selecting the neighbor nodes ‘$N_1, N_2, ..., N_n$’ and sends the event ‘$E$’ to the sink node ‘SN’. The Group based Collaborative Neighbor Selection function is formalized as given below

$$GCNS = (S_1, S_2, ..., S_n) \cup (R_1, R_2, ..., R_n) \rightarrow (N_1, N_2, ..., N_n)$$  \hspace{1cm} (1)

Time-efficient Sink Detection algorithm

The BO-GIDF framework employs Time-efficient Sink Detection algorithm to increase the network security and improve packet transmission. Each
source node is assigned with a specified time and according to that specified time the packet is send from the source node to the neighboring node.

If the destination node is nearer, the sensor nodes directly transfers or broadcasts the packets to it without the support of any other neighboring nodes. Moreover, the data aggregated and forwarded packets are secured through Time-efficient Sink Detection algorithm.

**Algorithm 1 – Time-efficient Sink Detection**

Step 1: Detection of an event ‘E’ by group source nodes S_1, S_2, ..., S_n with time of occurrence of event ‘T’ with time for each node set as ‘τ’

Step 2: Select the neighbor nodes ‘N_1, N_2, ...., N_n’

Step 3: Send the detected event ‘(E, P, T)’, with router information ‘R_1, R_2, ..., R_n’

Step 4: if source nodes consider event E as true and τ < T

Step 5: SD = (E, P)

Step 6: else

Step 7: SD discard the event ‘E’

Step 8: end if

Step 9: Check the existence of N_i(E_i, P_i)

Step 10: if (E_i, 1 ≤ i ≤ N_i) then consider the packet to be secured, else

Step 11: Discard the packet other wise

Step 12: end if

Step 13: end

Output Secured data aggregated and forwarded packets

**Associative Filtering scheme**

In large scale wireless sensor network, detecting events injected by compromised mobile sensor nodes is a large research confront. Once a mobile node is compromised, all the security aspects become accessible to attackers. In such sensor network, an improved authentication scheme is designed and developed to improve the security level at minimum time interval by efficient filtering of group injecting false data. BO-GIDF concentrates on removing the group injected false data attack and a mitigation scheme is designed for providing security at minimum processing time. The detected events are then verified in BO-GIDF framework and the group injected false data is effectively filtered through router nodes. As a result, the overhead at the sink node is reduced resulting in reducing the overall processing time of the sink node to identify the group false injected data in wireless sensor network.

**Network authenticated based on elgamal cryptography framework**

Network Authenticated based on ELGamal Cryptography is designed with the objective of minimizing the false data injection and therefore improving the security. The NAEC framework is designed on the basis of an asymmetric key encryption algorithm that helps in avoidance of false data injection. With this, the encrypted data isolate the malicious adversaries from injected false data present in the data packets during communication between the sensor nodes. The presence of malicious adversaries in the network is recognized by applying Diffie–Hellman key. Finally, an Implicit Authorized Certificate Rule is applied in this work with the objective of maintaining high degree of interoperability.

**ELGamal encryption algorithm**

ELGamal encryption algorithm is employed for securing distributed storage and transmission of data packets in wireless sensor network. ELGamal encryption algorithm minimizes the false data injection and therefore improving the rate of security. ELGamal encryption system is an asymmetric key encryption algorithm used for maintaining the network system with the avoidance of false data injection. The ELGamal encryption uses a homomorphic mapping model to improve the security during data packet transfer. With this the malicious adversaries are removed. Finally, mapping is performed for multiples of generator position. Therefore the false data injection in the data packet is reduced in an extensive manner. The encrypted data with private key structure easily isolate the malicious adversaries from the data packets (i.e., injected false data). ELGamal encryption enhanced privacy level with optimal strategy result on maintaining the Wireless Sensor Network Security.

**Diffie–Hellman key exchange model**

Diffie–Hellman key exchange model establishes symmetric keys between sensor nodes and a sink node. The Diffie–Hellman key exchange algorithm
includes three main steps. Initially, it obtains an agreed based point for the sensor nodes to establish communication and sent data packets between each other. Next, it generates a secret number for two sensor nodes separately and finally it evaluates the public point. Therefore, the processing time in identifying the malicious adversaries is reduced significantly. The encrypted data with private secret key structure easily isolate the malicious adversaries from the data packets (i.e., injected false data). The malicious adversaries in different structure are easily recognized when it does not satisfy the Diffie–Hellman key exchange form. Therefore, the processing time in identifying the malicious adversaries is reduced in an extensive manner.

Implicit Authorized Certificate Rule
Implicit Authorized certificate Rule is designed to avoid the injection of false data (i.e., threats) on dynamic paths. The certification of the sensor network system maintains high degree of interoperability. Malicious node’s max-min strategy on this authentication system is evaluated using the implicit authorized certification rule. The certificate authority selects a random number by the product of base point.

Algorithm 2: Implicit Authorized Certificate algorithm
Output: Interoperable authenticated sensor nodes
1: Begin
2: For every sensor node ‘SN_i’
3: Generate random number ‘p’
4: Evaluate ‘pBP’
5: Send to ‘CA’
6: ‘CA’ Select random number ‘n’
7: Evaluate ‘nBP’
8: Evaluate α = pBP * nBP
9: Assign sensor node ‘SN_A’ public key as α
10: If (SN_i == SN_i+1) then
12: End if
13: If (SN_i <> SN_i+1) then
14: Do not issue “Implicit Authorization Certificate”
15: End if
16: End for

The product of the two values obtained is then sent as the public key to the sensor node. If both the public key of the two sensor nodes are same, then Implicit Authorization Certificate is issued by CA and proceeds with data packet transfer. As a result, high degree of interoperability is maintained.

Resource usage control based packet data watermarking mechanism
Resource Usage Control based Packet Data Watermarking mechanism is designed to avoid false data injection in WSN. With the application of watermarking procedure, it control the time of accessing the resources and also reduces the resource utilization level. By using the changeability of packet data attributes set, resource utilization level is effectively maintains which in turn reduces the resource utilization. The RUCPDW mechanism using watermarking procedure performs the following process for enhancing the security in multipath transmission. The process involved in RUCPDW mechanism is as follows, network initialization, node authentication, authorized packet generation and authenticity verification.

Initialization Process
The first process performed in design of RUCPDW mechanism is initialization process where sensor nodes are deployed with base station. During the initialization process, each node in a sensor network allocated by the Base Station (BS) . At the same time, the BS will assign an arbitrary function that used for generating random numbers utilized in authorized packet generation. The BS in sensor network is used to handle the entire random function seed list. When transmitting the data, every node performs the following two functions, namely, one-way function and random functions. It is used to compute the watermark and to determine the random number.

Node Authentication Process
Node Authentication Process is the second mechanism in RUCPDW. After the sensor network positioned, Node Authentication Process is carried out for verifying whether the data is delivered to the exact node. During Node Authentication Process, base station sends a request to cluster head. The cluster head inform the nodes, to send the gathered data to the head node and then the cluster head aggregate the received sensor data, the authorized node will
generate verified watermark and send it with the serial number of the key to the cluster.

**Authorized Packet Generation**

After performing the Node Authentication Process, Authorized Packet Generation is carried out for transmitting the data to authorized node in sensor network. During watermarking embedding process, the data is watermarked and additional information is embedded to the watermarked data. When the watermark embedding is accomplished, the cluster head assigns the serial number are assigned by key and the timestamp into the data. This process are carried for avoiding the replay attacks which in turn significantly improves the security of data transmission in RUCPDW mechanism.

**Authenticity Verification**

The final process performed in design of RUCPDW mechanism is Authenticity Verification. This final process verifies the accuracy and authenticity of received data. During this process, RUCPDW mechanism is checks the timestamp to identify the repeated packets which results in reduced resource utilization. Then, RUCPDW mechanism the extracted watermark with the detect watermark compared to verify the authorized packets which results in improved security in multipath packet transmission. The extracted watermark is obtained from the received data and watermark is calculated by data characteristics and additional information.

**Algorithm 3-Processing steps of resource usage control**

```
Begin
//initialization process
Step 1: Sensor nodes are deployed with base station ‘BS’
Step 2: For each node
Step 3: BS will assigns the unique crypto key, node serial number, modulation value of difference expansion // Node Authentication Process
Step 4: BS sends a request to cluster head
Step 5: Cluster node sends the gathered data to Cluster head
Step 6: Cluster head performs data aggregation to obtain ‘D’
Step 7: cluster head selects ‘n’ nodes as authorized and sends a watermark request, most significant part (MSP) of aggregate data to each authorized node
Step 8: authorized nodes are compares the MSP with its gathered data to decide
   if (aggregate data is legitimate) then
   Step 9: Authorized node generate verified watermark to cluster head
   Step 10: Else
   Authorized node rejects to send verified watermark
   End if
   // Authorized Packet Generation
Step 11: compute watermark information
Step 12: determine the random number
Step 13: perform watermark embedding for transmitting the data to node
   // Authenticity Verification
Step 14: BS verifies the accuracy and legitimacy of received data
Step 15: checks the timestamp to identify the repeated packets
Step 16: compare extracted watermark with detect watermark to verify authenticity of the packet or data. End
```

With the application of watermarking procedure in RUCPDW mechanism, the packet data is forwarded to the destination end, watermarks. Security is ensured in the sensor network with resource efficient way of the data packet forwarded without any false data. Watermarking with the logical property in RUCPDW mechanism broadcast the information without malicious adversaries on multipath route.

**Experimental results**

NS-2 simulator used with the network range of 1200*1200 m size. For experimental purpose the number of sensor nodes selected. To perform data packet transmission moving speed is about 10 m/s for every sensor node with a simulation rate of 50 milliseconds is defined. The performance is evaluated using the parameters namely, resource utilization efficacy and packet transmission time. The simulation results are compared with BO-GIDF framework, NAEC framework and RUCPDW mechanism. Table 1, report the results that improves the Resource Utilization Efficacy and reduces the packet transmission time. Here, the RUCPDW mechanism improves the resource utilization efficacy
and BO-GIDF framework reduces the time taken for packet transmission while comparing with other state-of-methods. From the figure 3, Resource Utilization Efficacy using RUCPDW mechanism is higher. With the help of Watermarking procedure, repeated packets are identified and therefore improve the Resource Utilization Efficacy. When proposed RUCPDW mechanismis compared with existing method, resource utilization efficacy is improved by 20%. Similarly, other proposed BO-GIDF framework and NAEC framework, improves resource utilization efficacy by 8% and 15%. Therefore, RUCPDW mechanismimproves better resource utilization efficacy when compared with other start-of-methods. From figure 4, packet transmission time is reduced in BO-GIDF frameworkby applying this Time-efficient Sink Detection algorithm. When proposed BO-GIDF frameworkis compared with existing method, packet transmission time is reduced by 15%. Similarly, other proposed NAEC framework and RUCPDW mechanism, reduces packet transmission time by 10% and 6%. Therefore, BO-GIDF frameworkprovides better packet transmission time when compared with other start-of-method

**Conclusion**

A Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) framework overcomes the difficulty of group injected false data. It identifies the neighboring nodes during packet transmission in Wireless Sensor Network. Group based Collaborative Neighbor Selection scheme using the mobile compromised node that increases the bandwidth consumption efficiency. Network Authenticated based on ElGamal Cryptography (NAEC) framework is provided based on the Diffie–Hellman key exchange model. By applying the Diffie–Hellman key exchange in NAEC framework, reduces the processing time in identifying the malicious adversaries. Finally, Implicit Authorized certificate Rule is performed between the sensor nodes to maintain the high rate of interoperability. Resource Usage Control based Packet Data Watermarking mechanism improves the security in multipath data transmission with minimum resource utilization. By using the watermarking procedure in RUCPDW mechanism, packet data forwarded to the destination end. Initially, watermarks the data into lightweight system with objective of minimizing the energy consumption and improving the security.

**References**