International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 30249-30266

http://www.ripublication.com

Collabarative Neighbor Based Associative Filter For Secured Wireless Sensor Network

Mrs. L. Devi
M.C.A.,M.Phil., Ph.D,Reseacrh scholar
Bharathiar University, Coiambatore
Dr. S. P. Shantharajah
M.C.A.,Ph.D., Professor, Dept.of Computer Applications
Sona College of Technology, Salem

Abstract

Injecting false data attack is a well studied topic in Wireless Sensor Networks. Traditional bandwidth efficient mechanism filters the false data injection with minor extra overheads at the en-route nodes and reduces the energy in the entire network. But bandwidth efficient mechanism fail to prevent early detection of gang injecting false data attack from mobile compromised sensor nodes. An effective strategy for early detection of injected false data is to use data aggregation and data authentication protocol that can sparsely minimize the waste of resources including bandwidth and battery power for confidential data transmission. However, such data transmission framework did not address important factors such as network security and efficiency. In this paper, we present a localized Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) framework that handles group injected false data and improves network security by formulating a neighbor selection mechanism to identify whether the node is injected with false data or not. The BO-GIDF framework includes Group based Collaborative Neighbor Selection and time taken on packet forwarding from one point to another to identify the presence of false data being appended in the framework. With the application of Time-efficient Sink Detection algorithm, the occurrence of time event on packet forwarding helps to improve packet transmission. The proposed framework includes enhancement to security and efficiency by forwarding the node information and performing the verification procedure based on the received packet to filter the false data. We also demonstrate how the proposed framework can be extended to filter group of injected false data in the sensor network using Associative Filtering scheme. Extensive experiments and simulation results indicate that, in terms of bandwidth efficiency (for gang injecting false attack), packet transmission, network security and processing

time, BO-GIDF performs favorably compared to existing filtering mechanisms in wireless sensor network.

Keywords: Wireless Sensor Networks, Data aggregation, Data authentication, Data transmission, Collaborative Neighbor Selection, Security

Introduction

The sensor nodes in WSN communicate with the physical world at an extensive level to provided advantages to several new applications. However, the network is said to be hampered internally in an intentional manner in a hostile condition due to the sensor node failures accidentally. Also false data are said to be through via mobile compromised nodes, resulting in false alarms in WSN. In Bandwidth Efficient Cooperative Authentication (BECAN) [1], early detection of filtering was made possible through bit-compressed authentication technique with additional overheads at the routing. This in turn reduces the energy during routing at entire network.

Data Aggregation and Authentication (DAA) [2] mechanism was designed with the objective reducing energy by measuring small size message authentication codes during data verification and ensured security. However, early detection of false injecting data attack at group level was compromised. Random Graph and Bit Compromised Authentication techniques were used in [3] with the motive of preventing false data attack at group level. This helped in improving the efficiency of the network with reduced network overhead. But, attack with respect to mobile compromised nodes remained unaddressed. A good tradeoff was provided in [4] by addressed miss detection probability and false alarm through entropy-based trust model.

Many research works conducted on data aggregation in wireless sensor network made use of the trusted aggregator, and therefore the privacy of user against untrusted aggregator was not ensured. Bidirectional communication was ensured in [5] to address the issues related to untrusted aggregator. Though communication overhead was reduced, but at the cost of security. Ensuring security for mobile sensor nodes was the objective behind the design of Smart Grid in [6]. But, security against false data injection remained unsolved.

In [7], filtering methods were introduced to secure the network against false data injection in wireless sensor networks by using Hybrid Authentication Scheme (HAS). But there arise a tradeoff between security and time for event detection. With the application of Fuzzy values [8], accuracy was improved during event detection and also helped to reduce the size of rule being generated. The effect of temporal constraints remained unaddressed. In [9], distributed scheme was introduced with the objective of improving the efficiency and effectiveness on the probability of event being detected of false data injection in WSN.

Based on the above reviews made regarding false data injected in group scenario, in this work, we design a framework called, Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) that efficiently handles group injected false data. The contributions of BO-GIDF include the following:

- To improve the bandwidth efficiency rate by applying Group based Neighbor Collaborative Selection model.
- To enhance the packet transmission rate by designing a Time efficient Sink Detection algorithm
- To improve the network security in an extensive manner based on the event detection with the aid of neighboring sensor nodes.
- To reduce the processing time of group injected false data in Wireless Sensor Network with the application of Associative Filtering scheme.

This paper is structured as follows. Section 2 presents the related work. Section 3 presents our framework and the design of framework through neat diagrams. Section 4 includes the experimental setup with parametric definitions. Section 5 presents simulation results. Section 6 concludes with conclusions.

Related Works

In recent years, one of the significant foci in WSN is the address of false reports being injected by compromised nodes and the measures taken to detect such false reports. Cluster based Authentication Scheme (BAD) [10] provided measures to address false reports being entering into the network through cooperative authentication mechanism. This resulted in high filtering capability by reducing the energy in an intermittent manner. However, detection of multiple attacks was not provided.

In [11], Statistical En-route Filtering (SEF) was introduced using Localized Encryption and Authentication Protocol (LEAP) with the main aim of improving the security and reducing the energy during detection. However, robustness against various attacks remained unaddressed. Probabilistic Voting based Filtering Scheme (PVFS) [12] was designed using Fuzzy logic system to improve the energy saving during data transmission through neighbor nodes. However, optimal solutions were not provided.

To address optimality in [13], Locality based Distributed Search System was introduced to address the optimality by applying partial replication algorithm. Scalability and routing overhead was addressed in an optimal manner. However, false alarm rate was not reduced. To minimize the false alarm rate and improve the accuracy of the compromised nodes being detected, Support Vector Machine with online outlier detection techniques [14] was introduced.

Due to the nodes in wireless sensor network are broad in nature, false data injection is very hard to be detected. Bloom filter based Source Authentication (BSA) [15] was introduced to address the computational and communication overhead during false data injection with the aid of public key cryptography scheme. Identification of false event in the presence of compromised nodes was constructed in [16] with the objective of improving the security. Though security was ensured, with the increasing mobile sensor nodes, efficient measures were not taken to avoid false injection of data. En-routing filtering mechanisms [17] were introduced to address the scalability issues during false data injection through statistical measures.

Several filtering techniques were integrated in [18] to address the issues related to false data injection in WSN by ensuring security through hop-by-hop authentication

scheme. Another method called, Proportional integration synchronization was designed in [19] to reduce the communication overhead and improve performance degradation during injection of false data in group manner. To reduce the amount of data being transmitted to prevent false data injection, integration of secure data aggregation was introduced in [20].

Based on the aforementioned methods, in this work an efficient framework called, localized Bandwidth Optimal Group Injected Data Filtering is designed in the forthcoming section.

Design of Localized Bandwidth Optimal Group Injected Data Filtering

In this section, we briefly explain a localized Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) framework for preventing group injecting false data attack from mobile compromised sensor nodes and improve network security in Wireless Sensor Network (WSN). Due to the unattended or hostile environments in WSN, our main objective is to identify the group injecting false data attack and prevent mechanism by effective filtering method.

The goal of BO-GIDF framework is 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.

The sensor nodes in wireless sensor network are highly susceptible to group injecting of false data attack. This in turn affects the entire network that reduces the bandwidth and security breach. Figure 1 shows the workflow of our proposed framework with the objective of improving the bandwidth efficiency and increasing the network security in WSN. The proposed framework, BO-GIDF includes three parts, namely, construction of Group based Collaborative Neighbor Selection, an algorithm called, Time-efficient Sink Detection and design of Associative Filtering scheme.

Given a group of sensor nodes in WSN, we first obtain the source node, the packet to be transmitted and identify the neighboring nodes. The efficient neighbor node identificiation is performed by applying Group based Collaborative Neighbor Selection with the motive of increasing the bandwidth efficiency. Mobile compromised sensor node is identified on the basis of time of occurrence of event. Next, by applying the Time-efficient Sink Detection algorithm, network security and packet transmission is improved by observing the difference between the time interval and specified time.

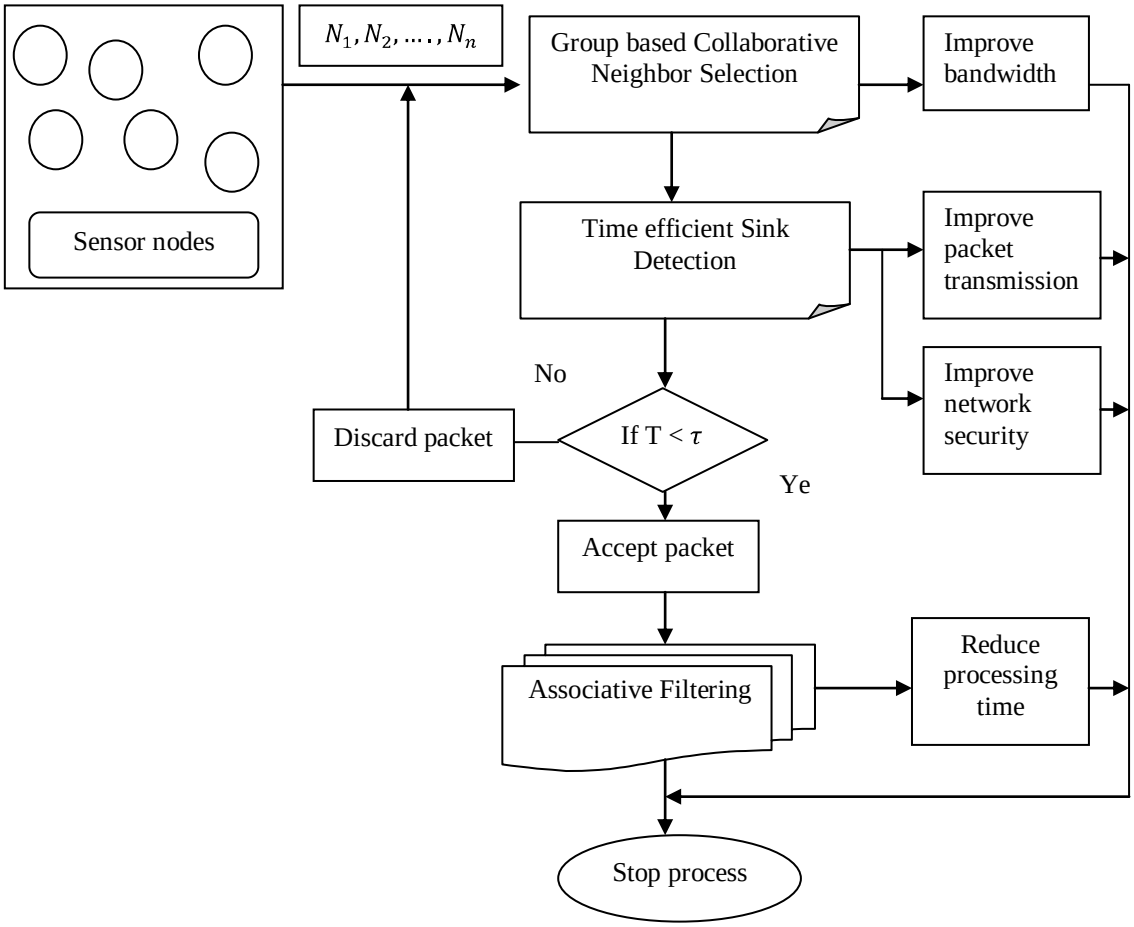

Figure 1: Workflow of Localized Bandwidth Optimal Group Injected Data Filtering

Finally, the processing time for identifying the group false injected data in wireless sensor network is reduced based on the different mobile source nodes and their packet size. Only, the source nodes with different packet size and same neighbor nodes or same packet size with different neighbor nodes are confirmed as valid source nodes whose packets are transferred to the sink node.

Group based Collaborative Neighbor Selection (improve bandwidth efficiency)
The framework localized Bandwidth Optimal Group Injected Data Filtering uses Group based Collaborative Neighbor Selection mechanism to mitigate against group injecting false attack from mobile compromised sensor nodes. The objective behind the application of Group based Collaborative Neighbor Selection (GCNS) mechanism is to improve the bandwidth efficiency by identifying whether the node is injected with false data or not in WSN. To filter the group injected false data from mobile compromised sensor nodes the BO-GIDF applies GCNS mechanism.

Figure 2 shows the design of GCNS mechanism when a source node '$S_1, S_2, \ldots, S_n$' identifies certain event 'E'. In the figure, the source node $S_2$is compromised and so it is said to be mobile compromised sensor node. The mobile compromised node is

obtained according to the movement of the sensor node from one position to another within the time the routers are identified for sending the packet information to the sink node.

$$MCN = \{S_i, S_{i+1}, \dots, S_{i_n-1}\} \rightarrow S_{i+1,i+1} \quad (1)$$

In (1), the occurrence of mobile compromised node 'MCN 'is obtained if the sensor node is moved from one place 'S_{i+1}' to another '$S_{i+1,i+1}$'.

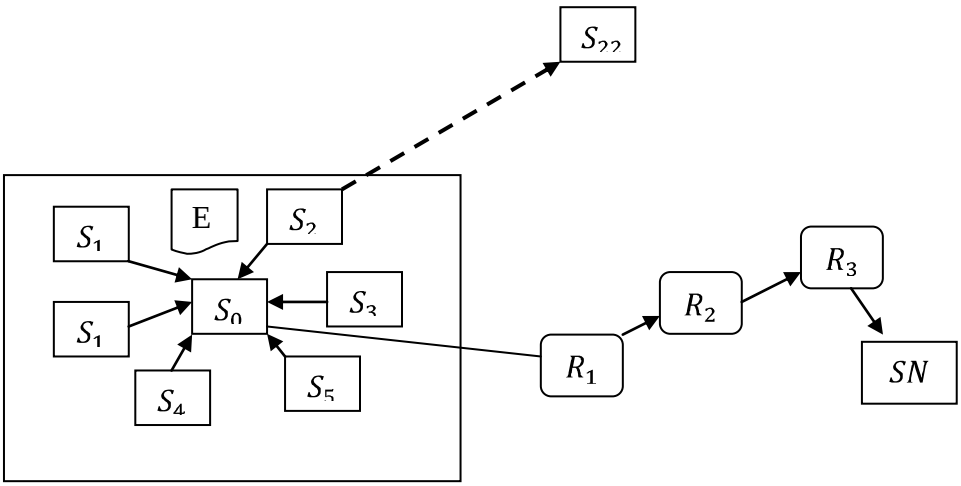

Figure 2: Construction of Group Based Collaborative Neighbor Selection

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 '$R_1, R_2, \dots, R_n$'. With this, the source node (i.e., group node) '$S_1, S_2, \dots, S_n$' obtains the time of occurrence of event 'T', by selecting the neighbor nodes '$N_1, N_2, \dots, N_n$' and sends the event 'E' to the sink node 'SN'. The Group based Collaborative Neighbor Selection function is formalized as given below

$$GCNS = (S_1, S_2, \dots, S_n) \cup (R_1, R_2, \dots, R_n) \rightarrow (N_1, N_2, \dots, N_n) \quad (2)$$

Once the sink node obtains the information (E, P, T), the framework BO-GIDF checks the packet integrity with the help of the packet 'P' and the time of occurrence of event 'T'. According to the results of the time of occurrence of event, if the time is obsolete, the message (P, T), is rejected or packet transmission occurs. On the other hand, the sink node call forth Time-efficient Sink Detection algorithm which is elaborated in the forthcoming section. This helps in improving the efficiency of bandwidth that in turn increase the average rate of successful packet transfer through different routers in WSN.

Time-efficient Sink Detection algorithm (improves packet transmission & network security)

Once the construction of Group based Collaborative Neighbor Selection is accomplished, the framework BO-GIDF employs Time-efficient Sink Detection algorithm to increase the network security and improve packet transmission.

Compared to Data Aggregation and Authentication protocol [2] that extracts false data by both data aggregation and data forwarding, network security is compromised in the network, proposed framework provides network security via TSD algorithm.

Each source node is assigned with a specified time and according to that specified time the packet is transferred from the source node to the neighboring node. If the TSD algorithm returns "acquire," the sink node accepts the packet. Otherwise the sink node rejects the packet. The design of Time-efficient Sink Detection is shown in figure 3.

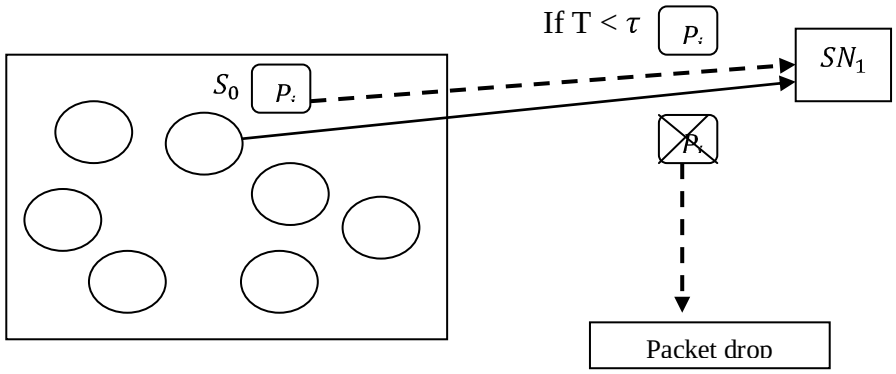

Figure 3: Design of Time-efficient Sink Detection

As shown in figure, time-efficient sink detection is constructed. When a source node 'S_0' wants to send a packet 'P_i' to the sink node, the time interval is checked with the specified time 'T'. The packet is received at the sink node when the time interval is less than the specified time, or it is discarded.

// Algorithm – Time-efficient Sink Detection

Step 1: Detection of an event 'E' by group source nodes $S_1, S_2, \dots, S_n$ with time of occurrence of event 'T' with time for each node set as 'τ'
Step 2: Select the neighbor nodes '$N_1, N_2, \dots, N_n$'
Step 3: Send the detected event '(E, P, T)', with router information '$R_1, R_2, \dots, R_n$'
Step 4: if source nodes consider event E as true and $\tau < T$
Step 5: $SD = (E, P)$
Step 6: else
Step 7: SD discard the event 'E'
Step 8: end if
Step 8: Check the existence of $N_i(E_i, P_i)$
Step 9: if $(E_i, 1 \leq i \leq N_i)$ then consider the packet to be secured, else
Step 10: Discard the packet other wise
Step 11: end if
Step 12: end
Output Secured data aggregated and forwarded packets

Algorithm 1 Time-efficient Sink Detection

The above algorithm, TSD provides the sink node to either obtain the event or discard the event, if it is considered to be false injected data. Sensor nodes in Wireless Sensor Network broadcast the packets to the destination nodes through the sink nodes. 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. On the other hand, if the distance between the source node and destination node are higher, then it has to be broadcasted through neighboring sensor nodes which it turn sends the packets to the sink node.

Whenever an event is detected by group of sensor nodes, the time of occurrence of event is noted in BO-GIDF. The occurrence of time event on forwarding from one neighbor node to another neighboring helps to easily recognize whether false data is appended in the system or not. As a result, whenever the time occurrence of event exceeds the specified time interval 'τ', the event E_i and corresponding packet $P_i$is considered as false detected and are discarded from the network. If the time occurrence of event is lesser than the specified time interval, the router forward the packets to other routers and then finally to the sink node. Efficient packet forwarding through router nodes via TSD is formalized as given below

$$PF_i = R_1 \cup R_2 \cup R_3 \ldots\ldots \cup R_n \tag{3}$$

In this way bandwidth efficiency is maintained using Group based Collaborative Neighbor Selection mechanism. Moreover, the data aggregated and forwarded packets are secured through Time-efficient Sink Detection algorithm.

Design of Associative Filtering scheme (minimizing process time to identify the group false injected data)

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.

The framework, BO-GIDF concentrates on removing the group injected false data attack and a mitigation scheme is designed for providing security at minimum processing time. Upon completion of Time-efficient Sink Detection algorithm based on time factor, the detected event (E, P, T), is sent to the sink node through routers. The detected events are then verified in BO-GIDF framework and the group injected false data is effectively filtered through router nodes. The router verifies the detected event using the occurrence of time event and accordingly verifies it. According, to the validity and integrity of the events being detected, it is either dropped or sent to the sink node.

In case of group verification of injected false data, when two different mobile source nodes send different events being detected to the sink node and if these mobile sources node has same cooperative neighbor node by generating the events at the

same time, then the size of the packet is verified for two different mobile source nodes.

Let us consider that two different mobile source nodes 'S_0' and 'S_1' wants to send the packets 'P_0' and 'P_1' with same neighbor node 'N_1', 'N_2' and 'N_3'. If the size of the packet is also said to be same, then the Associative Filtering in BO-GIDF framework states that any of these source node has been compromised with its neighbors. Then the router drops these two different mobile source nodes 'S_0 and S_1'. 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.

Experimental Setup

Localized Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) framework in wireslss sensor network uses the NS-2 simulator with the network range of 1000*1000 m size. The number of sensor nodes selected for experimental purpose is 70 nodes using Random Way Point (RWM) model for BO-GIDF framework. Destination Sequence Based Distance Vector (DSDV) is used as routing protocol to perform the experimental work.

The BO-GIDF framework's moving speed of the sensor nodes in WSN is about 3 m/s for each sensor node with a simulation rate of 40 milliseconds to perform single packet transfer from source to sink node. The values of each parameters for performing experiments are shown in table 1. Experiment is conducted on the factors such as bandwidth efficiency, packet transmission, network security and processing time for identifying group injected false data attack in WSN. The results of the metrics of BO-GIDF framework is compared against the existing methods such as Bandwidth Efficient Cooperative Authentication(BECAN) [1] scheme and Data Aggregation and Authentication (DAA) [2] mechanism.

Table 1: Simulation Setup

PARAMETER	**VALUE**
Protocols	DSDV
Network range	1000 m * 1000 m
Simulation time	100 s
Mobility model	Random Way Point
Number of nodes	10, 20, 30, 40, 50, 60, 70
Network simulator	NS 2.34
Network load	4 packets/sec
Mobility speed	3 m/s
Pause time	10

Simulation Results

Performance Metrics

The performance of Localized Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) framework in Wireless Sensor Network is compared with the Bandwidth Efficient Cooperative Authentication(BECAN) [1] scheme and Data Aggregation and Authentication (DAA) [2] mechanism. The performance is evaluated according to the following metrics.

Bandwidth consumption using BO-GIDF measures the amount of data that can be transmitted in a fixed amount of time. It is measured in terms of bits per second (bps). The formulation of bandwidth consumption is given as below

$$B = No.of\ nodes * Data_T\ (KB) * Time(ms) \quad (4)$$

Packet transmission time using BO-GIDF is the amount of time taken to transmit packet including the size of the header at a specified speed.

$$PT_{time} = P_{size} * H_{size} * \frac{1}{speed} \quad (5)$$

Where P_{size}refers to the size of the packet, including the header size H_{size} and speed denoted by $speed$. It is measured in terms of milliseconds (ms).

The processing time for identifying group injected false data attack measures the difference between the start time and end time to identify the group based collaborative neighbor selection function. It is measured in terms of milliseconds (ms).

$$Time = Start\ time\ (GCNS) - End\ time\ (GCNS) \quad (6)$$

Scenario 1 : Performance comparison of bandwidth consumption

Table 2 represents the bandwidth consumption efficiency using NS simulator and comparison is made with two other methods, namely BECAN [1] and DAA [2]. Let us consider for 10 nodes, the data to be transmitted is 2 KB and the time taken to transmit 2 KB of data is 5 ms using BO-GIDF, 6 ms using BECAN and 8 ms using DAA. Then, the mathematical value for bandwidth consumption efficiency using the three methods, BO-GIDF, BECAN and DAA is given below:

B (using BO-GIDF) = 10 * 16000 (bits) * 0.005 (sec) = 800 bps
B (using BECAN) = 10 * 16000 (bits) * 0.006 (sec) = 960 bps
B (using DAA) = 10 * 16000 (bits) * 0.008 (sec) = 1280 bps

Table 2: Tabulation Factors For Bandwidth Consumption

No. of nodes	**Bandwidth consumption (bps)**		
	BO-GIDF	**BECAN**	**DAA**
10	810	965	1285
20	1585	1753	2381
30	2335	2650	3541

40	3045	3500	4713
50	3952	4480	5916
60	4732	5321	7130
70	5532	5580	8310

Figure 4 shows the result of bandwidth consumption efficiency versus the varying number of sensor nodes. To better perceive the efficacy of the proposed BO-GIDF framework, substantial experimental results are illustrated in Figure 4. The BO-GIDF framework is compared against the existing BECAN [1] and DAA [2].

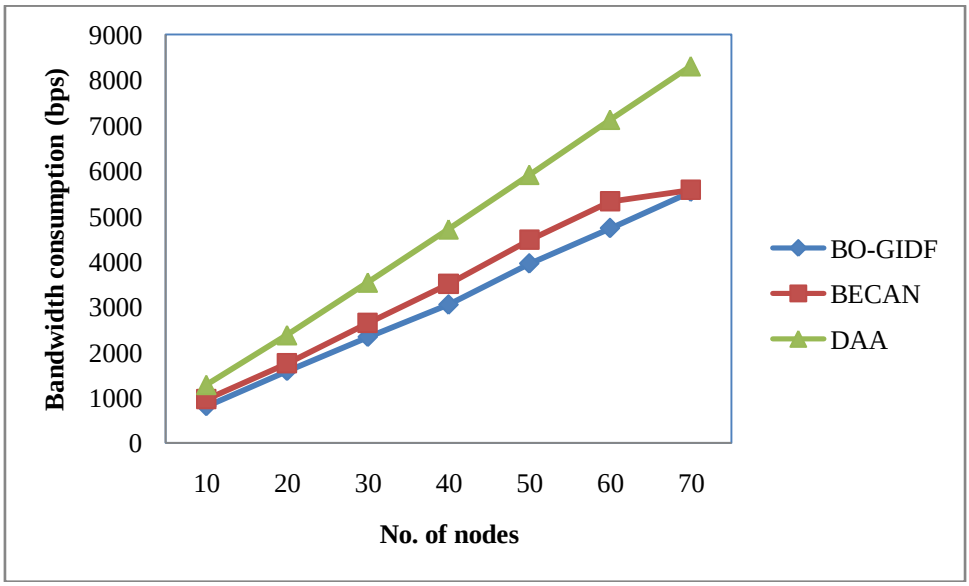

Figure 4: Measure Of Bandwidth Consumption Efficiency

Results are presented for different number of sensor nodes. The bandwidth consumption efficiency for group injected data filtering measures the amount of bandwidth consumed foe different sensor nodes. Higher, the number of sensor nodes, more successful the method is. The results reported here confirm that with the increase in the number of sensor nodes, the bandwidth consumption efficiency also increases. The process is repeated for 70 sensor nodes for conducting experiments. As illustrated in Figure 4, the proposed BO-GIDF framework performs relatively well when compared to two other methods BECAN [1] and DAA [2]. The framework had better changes using the extensive historic knowledge of the identification of Mobile Compromised Node. This is because in order to obtain the Mobile Compromised Node, the movement of the sensor node is based on the on the information collected from neighbor nodes or group based neighbor selection function. This in turn increases the bandwidth consumption efficiency in Wireless Sensor Network using BO-GIDF framework by 10 – 19 % compared to BECAN and 49 – 58 % compared to DAA respectively.

Scenario 2: Performance comparison of packet transmission time
As listed in table 2, the BO-GIDF framework measures the packet transmission time for sink detection which is measured in terms of milliseconds (ms). The packet transmissiontime using BO-GIDF framework offer comparable values than the state-of-the-art methods. Let us consider that the packet size is 400 bytes, including an header size of 40 bytes with the speed being 750 kbps using BO-GIDF, 780 kbps using BECAN and 800 kbps using DAA, then the packet transmission time for BO-GIDF, BECAN and DAA is given by

PT (using BO-GIDF) = (400 * 8)/750000 = 0.004266 = 4.3 ms
PT (using BECAN) = (400 * 9)/780000 = 0.00461 = 4.6 ms
PT (using DAA) = (400 * 10)/80000 = 0.005 = 5.0 ms

In order to reduce the packet transmission time with the increasing topological changes observed in WSN, the packet size for different nodes is considered. In the experimental setup, the packet size ranges from 400 bytes to 2800 bytes. The results for 7 packets of varying size are illustrated in figure 5. The packet transmission time using our framework BO-GIDF offer comparable values than the state-of-the-art methods.

Table 3: Tabulation Factors For Packet Transmission Time

Packet size (bytes)	**Packet transmission time (ms)**		
	BO-GIDF	**BECAN**	**DAA**
400	4.5	4.8	5.2
800	4.9	5.1	5.4
1200	5.3	5.5	5.8
1600	5.5	5.9	6
2000	5.0	5.2	5.5
2400	4.7	4.9	5.1
2800	4.5	4.7	4.75

The targeting results of packet transmission time for varying number of nodes with different packet sizes using BO-GIDF architecture and comparison made with BECAN and DAA are shown in figure 5.

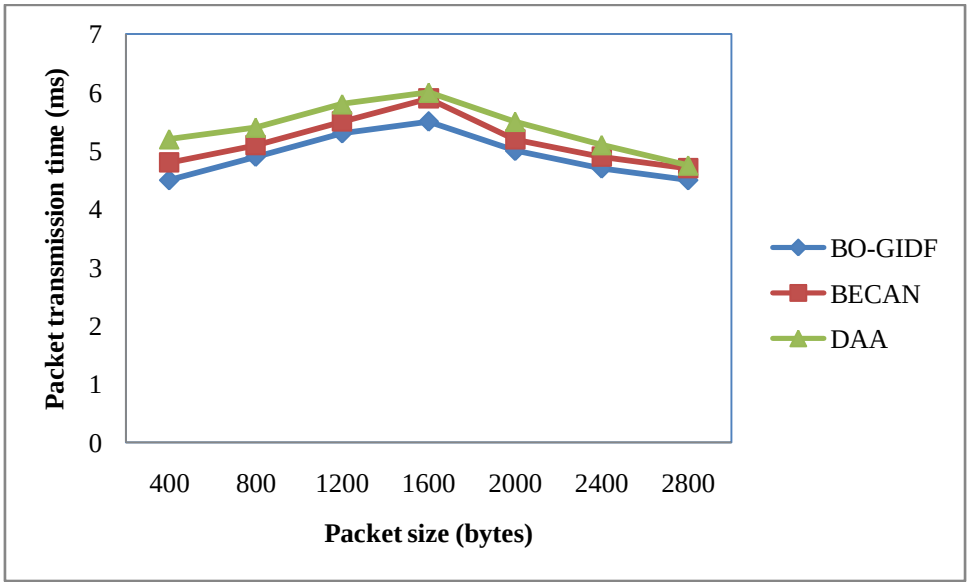

Figure 5: Measure of Packet Transmission Time

As shown in the figure, the proposed BO-GIDF framework offers comparatively lesser packet transmission time than the state-of-the-art methods. Our framework differs from the BECAN [1] and DAA [2] in that we have incorporated Time-efficient Sink Detection algorithm. By applying this Time-efficient Sink Detection algorithm, the occurrence of time event between the neighboring nodes are measured and compared with the specified time interval 'τ'. According to this 'τ', the router forward the packets to other routers and then finally to the sink node. This in turn helps in improving the packet transmission time using BO-GIDF framework compared to BECAN by 3 – 7 % and 5 – 15 % compared to DAA.

Scenario 3: Performance comparison of processing time for identifying group injected false data attack

In table 4 we further compare the processing time for identifying group injected false data attack in WSN using the BO-GIDF framework. The experiments were conducted using seven test cases in the range of 10 to 70 that measures the processing time in terms of milliseconds (ms). Let us consider that the starat time for group based collaborative neighbor selection function is 1.25 ms and end time is 0.70 ms using BO-GIDF, 0.65 ms using BECAN and 0.5 ms using DAA, then the processing time is given as below

Time (using BO-GIDF) = 10 * (1.25 – 0.70) = 5.5
Time (using BECAN) = 10 * (1.25 – 0.65) = 6
Time (using DAA) = 10 * (1.25 – 0.5) = 7.5

Table 4: Tabulation Factors For Processing Time

No. of nodes	Processing time (ms)		
	BO-GIDF	**BECAN**	**DAA**
10	5.8	6.2	7.8
20	6.1	6.5	8.2
30	6.5	6.9	8.5
40	6.2	6.8	8.2
50	6.8	7.2	8.8
60	7	7.4	9.2
70	6.6	7.1	8.9

Figure 6 given below shows the processing time for BO-GIDF framework, BECAN [1] and DAA [2] versus increasing number of nodes in the range of 10 to 70. The processing time returned over BECAN and DAA increases gradually as the number of nodes of nodes gets increased though not linear because of the topological changes and movement of neighboring nodes in WSN.

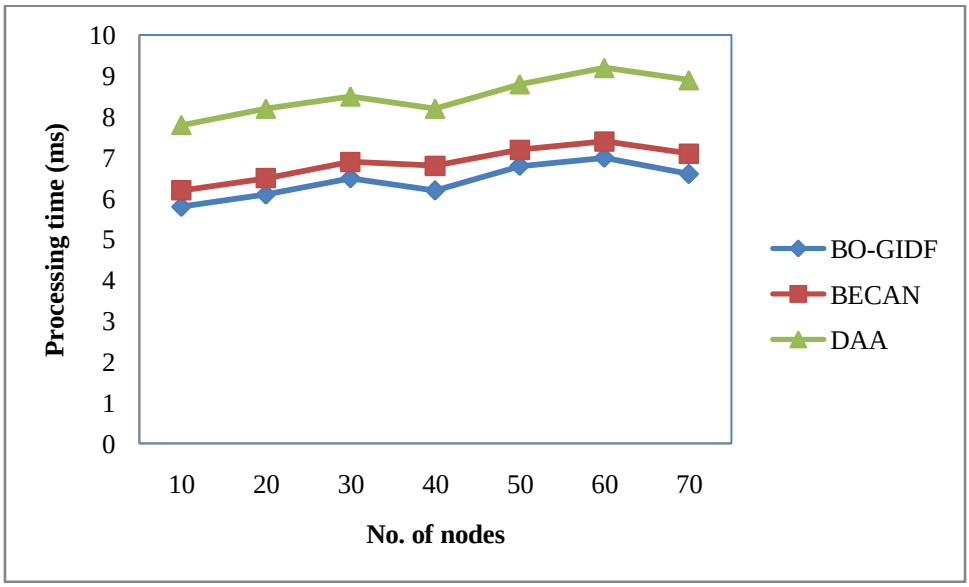

Figure 6: Measure of Processing Time

From figure 6, it is illustrative that the processing time is reduced using the proposed framework BO-GIDP. For example when the number of nodes is 10, the percentage improvement of BO-GIDP framework compared to BECAN is 6.89 percent and 34.48 percent compared to DAA, whereas when the number of nodes is 60 the improvements are around 5.71 and 31.42 percent compared to BECAN and DAA respectively. This is because of the application of Associative Filtering scheme in BO-GIDP, the detected events are sent to the sink node through router nodes. By verifying the size of the packets, the packets are either considered or droped using the

associative filter. Therefore, the overhead at the sink node is reduced, therefore reducing the processing time using the BO-GIDP framework by 5 – 9 % compared to BECAN and 29 – 34 % compared to DAA respectively.

Scenario 4: Performance Comparison of Security

Table 5 lists out the security provided by BO-GIDF framework and the two state-of-the-art methods [1] and [2].

Methods	**Security (%)**
BO-GIDF	83.45
BECAN	75.82
DAA	71.13

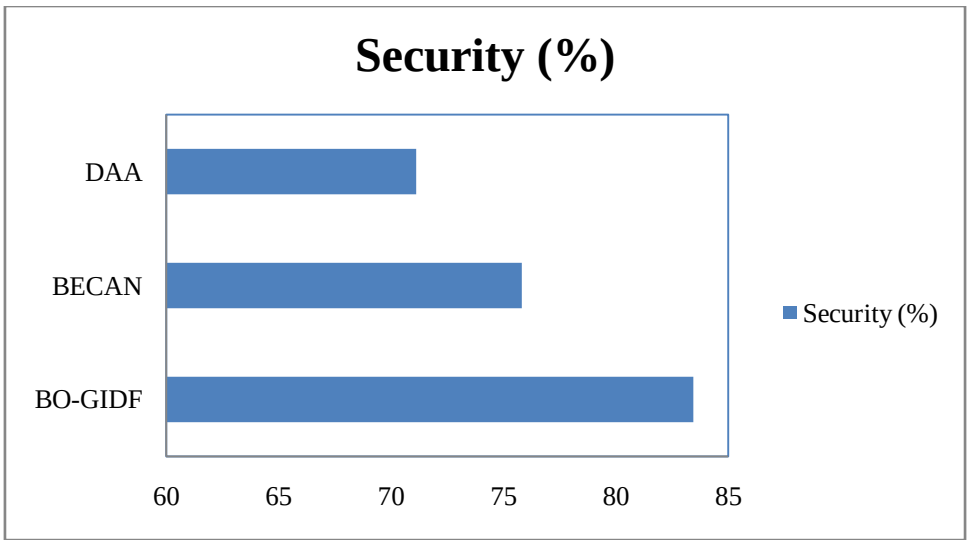

Figure 7: Measure of Security

Figure 7 shows the security provided by three methods, BO-GIDF, BECAN and DAA. From the figure, it is evident that the security is increased in the proposed framework BO-GIDF compared to BECAN and DAA. This is because by selecting the neighbor selection mechanism, whether the node is injected with false data or not is identified at an early stage and accordingly performs the verification process with less processing time. With the application of Time-efficient Sink Detection algorithm, removes the group injected false data, improving the security in BO-DIGF framework by 9.14 % in BECAN and 6.18 % in DAA.

Conclusion

A Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) framework to overcome the difficulty of group injected false data by identifying the neighboring nodes during packet transmission in Wireless Sensor Netowork is introduced. We

then showed how this framework can be extended to incorporate Group based Collaborative Neighbor Selection scheme to improve the bandwidth consumption efficiency by by identifying whether the node is injected with false data or not. Group based Collaborative Neighbor Selection scheme using the mobile compromised node increases the bandwidth consumption efficiency. Next, the introduced Tim-efficient Sink Detection algorithm works on improving the packet transmission and network security through the time occurrence of event by efficient packet forwarding. Finally, the design of Associative Fitlering scheme minimizes the processing time taken to identify the group false injected data in WSN. In our experimental results the Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) framework showed better performance than the state-of-the-art-works over the parameters, bandwidth consumption, packet transmission time, processing time and security in Wireless Sensor Network.

References

[1] Rongxing Lu., Xiaodong Lin., Haojin Zhu., Xiaohui Liang, and Xuemin (Sherman) Shen., "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. X, NO. X, XX 2010

[2] Suat Ozdemir., and Hasan Çam., "Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 18, NO. 3, JUNE 2010

[3] A. Mallareddy, P.Keerthi, D.Prathibha," Reducing the gang injecting false data attack from compromised Sensor nodes using random graph and bit compressed Authentication techniques", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 10, October 2014

[4] Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren, and Tongtong Li," Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 4, APRIL 2014

[5] Qinghua Li, Guohong Cao, and Thomas F. La Porta," Efficient and Privacy-Aware Data Aggregation in Mobile Sensing", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 2, MARCH/APRIL 2014

[6] Wenye Wang, Zhuo Lu," Cyber security in the Smart Grid: Survey and challenges", Computer Networks, Elsevier,Jan 2013

[7] Shahina K, Anand Pavithran," Filtering Schemes for Injected False Data in WSN", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 13, Issue 6, Aug 2013

[8] Krasimira Kapitanova, Sang H. Son, Kyoung-Don Kang," Using fuzzy logic for robust event detection in wireless sensor networks", Ad Hoc Networks,Elsevier, May 2011

[9] Qinghua Li, Wei Gao, Sencun Zhu, and Guohong Cao,," To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 3, MAY/JUNE 2013

[10] Uma Narayanan, Arun Soman," CAFS: Cluster based Authentication scheme for Filtering False data in wireless Sensor network", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[11] Su Man Nam and Tae Ho Cho," A METHOD FOR DETECTING MULTIPLE ATTACKS AGAINST FALSE REPORT INJECTION ATTACKS AND WORMHOLE ATTACKS IN SENSOR NETWORKS", Computer Applications: An International Journal (CAIJ), Vol.1, No.2, November 2014

[12] Jae Kwan Lee and Tae Ho Cho," ENSF: ENERGY-EFFICIENT NEXT-HOP SELECTION METHOD USING FUZZY LOGIC IN PROBABILISTIC VOTING-BASED FILTERING SCHEME", International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.4, December 2014

[13] Haiying Shen, Senior Member, IEEE, Ze Li, Student Member, IEEE, and Kang Chen," A Scalable and Mobility-Resilient Data Search System for Large-Scale Mobile Wireless Networks Haiying Shen, Senior Member, IEEE, Ze Li, Student Member, IEEE", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 5, MAY 2014

[14] Yang Zhang, Nirvana Meratnia, Paul J.M. Havinga," Distributed online outlier detection in wireless sensor networks using ellipsoidal support vector machine", Ad Hoc Networks, Elsevier, Oct 2012

[15] Syama M and Deepti C," AN EVALUATION OF ENERGY EFFICIENT SOURCE AUTHENTICATION METHODS FOR FALSE DATA FILTERING IN WSN", International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 2, April 2013

[16] Shimi K S,"Event Identificaiton for Wireless Sensor Network", International Journal of Scientific and Research Publications, Vol4., Issue.11, Nov 2014

[17] Syama M, Deepti C," An Evaluation Of En-Route Filtering Methods For False Data Injection Attack In WSNs", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 4, April – 2013

[18] FirozehEskandari and Mehdi Javanmard," Combining Filtering Techniquesin Wireless Sensor Network", Advances in Natural and Applied Sciences", AENSI Journals,Sep 2014

[19] KASIM S˙INAN YILDIRIM, RUGGERO CARLI, LUCA SCHENATO," Proportional-Integral Clock Synchronization In Wireless Sensor Networks", ACM Transactions on Sensor Networks,Oct 2011

[20] K. Panimalar, M. Priyadharshini, M. Abiya, S. Pushpalatchumy," FALSE DATA DETECTION AND SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS", International Journal of Computer Engineering & Science, Sept 2013