ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.11

An Efficient Secure Data Transmission & False Detection in Wireless Sensor Networks

R. Naveenraj
M.Phil Student
Department of Computer Science
Muthayammal College of Arts & Science, Namakkal, Tamilnadu, India

Abstract:
In the recent years, one among the most emerging technology is Wireless Sensor Networks which consists of thousands of small and low cost sensors. These sensors have limited power, computation, storage and communication capabilities. Communication among sensors consumes a considerable amount of energy and thus the amount of data transmission should be minimized in order to improve the lifetime of the sensors and effective utilization of the bandwidth. So data aggregation process is required which combines the data coming from various sensors, remove the redundancies in those data and then enroot them. However, this paper presents a data aggregation and authentication protocol, called DAA, to integrate false data detection with data aggregation and confidentiality. The DAA detects the false data injected by the up to T compromise node, and that the detected false data are not forwarded beyond the next data aggregator on the path. The experimental results shows that DAA can still reduce the amount of transmitted data by up to 60%with the help of data aggregation and early detection of false data.

Keywords: Data aggregation, data integrity, network-level security, sensor networks.

I. INTRODUCTION

Wireless sensor networks are undoubtedly one of the largest growing types of networks today. Wireless networks are facing many types of security attacks, including false data injection, data forgery, and eavesdropping. Sensor nodes can be compromised by intruders, and the compromised nodes can distort data integrity by injecting false data. The transmission of false data depletes the constrained battery power and degrades the bandwidth utilization. Much research has been done to make these networks operate more efficiently including the application of data aggregation. Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission, and improve data accuracy. Data aggregation results in better bandwidth and battery utilization, which enhances the network lifetime because communication constitutes 70% of the total energy consumption of the network. Although data aggregation is very useful, it could cause some security problems because a compromised data aggregator may inject false data during data aggregation. These papers introduce to detect the false data detection and secure data aggregation up to T compromise sensor nodes by using data aggregation and authentication protocol (DAA).In this paper is organized as follows.

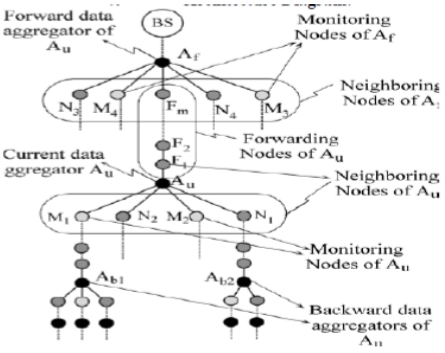

Fig 1 Architecture of DAA

Wireless sensor networks are vulnerable to many types of security attacks, including false data injection, data forgery, and eavesdropping [1]. The transmission of false data depletes the constrained battery power and degrades the band- width utilization. False data can be injected by compromised sensor nodes in various ways, including data aggregation and relaying. The existing false data detection techniques consider false data injections during data forwarding only and do not allow any change on the data by data aggregation. To support data aggregation along with false data detection, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small-size message.

II.RELATED WORK

Sensor nodes are often deployed in a hostile environment and it may be captured or compromised by the adversaries and secret information such as symmetric key may be revealed to the adversaries. Thus adversaries can easily inject false data reports of non-existing events or faked readings. Such an attack is called false data injection attack. It may not only cause false alarms due to bogus sensing reports but also drain out the limited energy of the nodes forwarding these reports, thus reduce the lifetime of the sensor networks. Three schemes have been proposed to detect and contain such attacks.SEF is a pre deployment scheme in which each node randomly picks some secret keys from one partition of a global key pool before deployment. All nodes have pre determined probability to detect and filter false report. It has limited filtering capacity. Hence a post deployment scheme that requires each node periodically establish pair wise keys with others that are multi hop away from it. This scheme can drop false report within the fixed number of hops. This requirement is impractical for the sensor network with high dynamic topological changes, which are due to nodes failures or nodes switching their state between active and sleeping mode to save energy.

Commutative Cipher based En-route Filtering (CCEF) scheme in which each node preloads a distinct authentication key before deployment. When the reports are needed the base station distributes a session key to the cluster head and a witness key to the forwarding nodes respectively. It suffers from dynamic topology problem by requiring the same fixed path from messages in both directions between the base station and the cluster head. Data aggregation usually involves the fusion of the data from multiple sensors at intermediate nodes and transmission of aggregated data to the base station. Data aggregation attempts to collect the most critical data from the sensors and make it available to the sink in an energy efficient manner with maximum data latency. The following issues have been addressed for secure data aggregation. Some sensor nodes may be compromised and transmit wrong data values to the aggregator that corrupts the aggregation result. The aggregator may be compromised and report maliciously aggregate values to the home serve or the sink. Estimation errors introduced by the sampling techniques used by the aggregator to compute the result.

III. METHODOLOGY

DAA protocol aims to integrate false data detection with the data aggregation and data forwarding. For every data aggregator the corresponding small-size MAC codes are computed and Data verification at the pair mates are made. For confidentiality, the data aggregators verify the data integrity on the encrypted data. DAA provides secure data aggregation, data confidentiality, and false data detection by performing data aggregation at data aggregators and their neighboring nodes and verifying the aggregated data. Data fusion is used to process the collected information before they are sent to the base station or the observer of the sensor network. The security of data fusion process is studied .Data fusion is employed in order to reduce the traffic load from the entire sensor to the base station. To reduce energy consumption in the scheme, minimum length needed for the message authentication code to achieve a ore defined level of security. The results show that the number of both used for MAC's does not increase linearly with the number of witnesses. Recent advances in wireless communication and electronics have enabled the development of low-cost, low power, multi functional sensor nodes that are small in size and communicate undeterred in short distances.

1. Data Detection

The design of sensor networks is influenced by many factors including fault tolerance, scalability, production cost, operating environment, sensor network topology, hardware constraints, transmission media and power consumptions. The main task of a sensor node in a sensor field is to detect events, perform quick local data processing and then transmit data. Power consumption can hence be divides in to three domains-sensing, communication and data processing. DAA protocol aims to integrate false data detection with the data aggregation and data forwarding. For every data aggregator the corresponding small-size MAC codes are computed and Data verification at the pair mates is made. For confidentiality, the data aggregators verify the data integrity on the encrypted data.DAA provides secure data aggregation, data confidentiality, and false data detection by performing data aggregation at data aggregators and their neighboring nodes and verifying the aggregated data during data forwarding between two consecutive data aggregators.

2. Network Topology:

This paper aims at providing network security and efficiency. The mainstay of our work is to integrate the False Data Detection with Data Aggregation and Confidentiality Using data. Aggregation and authentication protocol (DAA). Compromised sensor nodes can distort the integrity of data by injecting false data Previously known techniques on false data detection do not support data confidentiality and aggregation, even though they are usually essential to wireless sensor networks. However, our work has presented the novel security protocol DAA to integrate data aggregation, confidentiality, and false data detection. DAA appends two FMACs to each data packet. To reduce the communication overhead of algorithm SDFC, the size of each FMAC is kept fixed. Each FMAC consists of T+1 subMACs to safeguard the data against up to T compromised sensor nodes. Monitoring nodes are selected from the neighboring nodes that are present in the network using the MNS algorithm. Thus backward aggregators send the intended data.

3. Non-manipulabilit

A party's contribution in the election process should not be able to influence the decision of honest nodes towards the election of preselected nodes. We further call a protocol strongly non-manipulable, if in addition to the above property, no party has the ability to prevent the election of a preselected node. Unlike non-manipulability, strong non-manipulability is desirable but not required by a SANE protocol. Election protocol messages are exchanged only among nodes in the same sector. These messages are either sent via uncast among nodes in the same sector or disseminated to all nodes in a sector using a simple sector-aware controlled flooding scheme. With this flooding scheme, nodes re-broadcast first seen messages only if the source of the message belongs to the same sector as they do. We denote the i-th sensor node in a sector S by si, and the aggregator node during the t-th epoch as At. For each sensor si, we denote by Ni C S, the set of nodes from which it has received valid election contributions during an election round.

4. Authentication

Each party should consider only the contributions of a restricted set of nodes. Contributing nodes should be capable of proving that they belong to this set. We note here that our protocol descriptions do not explicitly address authentication, however this is a property that can be efficiently achieved by incorporating existing WSN authentication solutions.

5. Unpredictability

An election protocol is predictable if the adversary can forehand know the order in which nodes are elected as aggregators. This information could facilitate adversarial actions. For example, an adversary with the ability to compromise only a few nodes at a time could use this knowledge to prevent a cluster of sensor nodes from transmitting information to its consumer during selected periods.

IV. EXPERIMENTAL SETUP

In the existing system, it has been mentioned that DAA is simulated using QualNet network simulator for an area of

100*100 m and 100 sensor nodes with a transmission range of 15 m. Some nodes are designated as data aggregators and distributed into the network area uniformly. Data are assumed to be generated mainly by the nodes located at the edges of the network, although any node is allowed to sense events and generate data. But we implemented it using the Bluetooth concept which directly detects the neighboring nodes that have been created in individual systems so that it can be formed as a full network. By doing so the data transmission can be made from any node making it as a source and then to forward it to the desired destination, the concept can be extended easily. The data aggregator and all neighboring nodes are involved with the selection of monitoring nodes to minimize the adverse impact of a compromised node. MNS protects a compromised data aggregator from affecting the monitoring node selection. The monitoring nodes are selected by all neighboring nodes. To affect the selected monitoring nodes, a compromised data aggregator must change the random numbers before broadcasting them.

Assumptions Data aggregation and authentication protocol (DAA) are chosen three limitations:

Network topology: In this topology, there are at least nodes, called forwarding nodes, on the path between any two consecutive data aggregators; and each data aggregator has at least neighboring nodes, so they can form pairs with the forwarding nodes on the path between two consecutive data aggregators.

Generation of MACs: In DAA, only data aggregators are allowed to encrypt and decrypt the aggregated data from TinySec data packet structure [4] includes29-byte payload and a 4-byte MAC.

Group key establishment: Each data aggregator Au and its neighboring nodes are assumed to establish a group key, called kgroup, using an existing group key establishment scheme. The group key is used for selecting the monitoring nodes of the data aggregator, and protecting data confidentiality while data are transmitted among data aggregator and its neighboring nodes for data verification and aggregation. DAA provides secure data aggregation, data confidentiality, and false data detection by performing data aggregation at data aggregators. Monitor node selection: In this section, monitor node selection has performed secure data aggregation and to compute sub Macs of the aggregator are explained details Forming pairs of sensor nodes in wireless sensor network: Forming pairs of sensor nodes can perform false data detection and data confidentiality. The following 2T+1 pairs of nodes are formed. They are a) one AA-type pair are formed between current and forward data aggregator b) T pairs of MF-type pair are formed between monitor nodes of current data aggregator and forward nodes of forward data aggregator. c) T pairs of MN-type pair are formed between monitor nodes of current data aggregator and neighbor nodes of forward data aggregator as show fig 2.Here T represent as number of monitor nodes in each data aggregator and number of forward nodes=>T. To support data aggregation along with false data detection, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small-size message authentication codes for data verification at their pair mates Integration of secure data aggregation and false data detection (FDD): In this section, one AA-type pair computes the two FMAC for encrypted and plain text of each monitor nodes. T pairs of MN-type pairs are computed sub MACs of monitor nodes and T pairs of MF-type pairs are verifying the sub MACs of monitor nodes. Sub Macs for plain data are used for FDD during DA. Sub Macs for encrypted data are used for FDD during DF. This section introduces Algorithm SDFC to provide false data detection, secure data aggregation and data confidentiality for the third step of DAA. To provide data confidentiality, transmitted data are always encrypted and forwarding nodes perform the data verification over the encrypted data. Prior to this third step of DAA, monitoring nodes of every data aggregator are selected, and 2T+1 pairs are formed. To verify data integrity and detect false data injections, one pairmate computes a subMAC, and the other pairmate verifies the subMAC. subMACs are computed for both plain and encrypted data.

Table 1: Pair mates selection of DAA

1.	$A_f \rightarrow F_j \rightarrow A_u$	pairmate discovery message N_i's of A_f $MAC_{K_{i,u}}(N_i$'s) F_j's IDs for $1 \le j \le h$
2.	$A_u \Rightarrow T\ M_k$'s	$MAC_{K_{group}^u}(F_1 \mid \cdots \mid F_h)$ for new, random forwarding node labeling $MAC_{K_{group}^u}(N_i$'s)s
3.	$M_k \rightarrow A_u$	one forwarding node one neighbouring node
4.	$A_u \Rightarrow T\ M_k$'s	two pairmate lists of size T
5.	M_k	pairmate verification

Whenever some data are received by a data aggregator, the authenticity of data is verified by the data aggregator and its neighboring nodes; 2) The data aggregator and its monitoring nodes aggregate the data independently of each other; unlink able mention pre-diction, like the score of the top-ranked candidate and whether or not the entity mention is detected by some NER as a named entity. For the binary classifier, most systems use the SVM classifier. Each monitoring node computes one subMAC for the encrypted data and the other subMAC for the plain data; The data aggregator collects these subMACs from its monitoring nodes to form the FMACs of the encrypted and plain data, appends the FMACs to the encrypted data, and transmits them; The forwarding nodes verify the data integrity of the encrypted data; and The neighboring nodes of the next aggregator verify the integrity of the plain data. Each data aggregator forms two FMACs: one FMAC for the encrypted data, and the other FMAC for the plain data. Each FMAC consists of T+1 subMACs computed by the data aggregator Au and its T monitoring nodes. In the formation of FMACs, data aggregator Au determines the order of subMACs in anyway and inform each forwarding node about its subMAC location individually. For demonstrating the detail of effectiveness of proposed approach, Entity linking with knowledge base learning approaches.

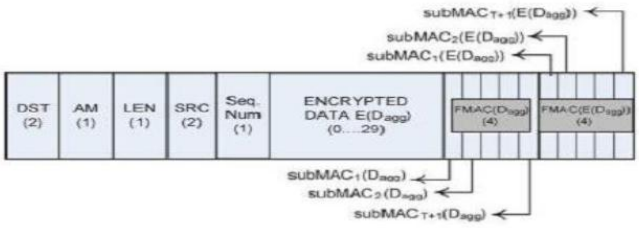

Fig.2: Packet structure of algorithm SDFC

Node Information

Node information displays the name of the node, the input that the user entered for each node. And it also displays the randomly generated memory, Battery life and mobility which

determine the strength of every node that is created in the network.

Aggregator Information
Based on the memory, battery and mobility that was generated earlier current aggregator is selected and displayed. The node that has the highest sum of these three gets elected. This is the node that connects the backward and forward aggregators for sending the intended information in the designed network.

Data Transfer Details Once nodes are created in the network, based on the range that is given to the nodes neighbors that are in close proximity to each other are detected and displayed. This also has the destination column to indicate the path via which information has to flow. The information is browsed and sent. To display this to the user, send and receive columns are used. The inject procedure is used for sending the malicious data in the network.

Selection Of Monitoring Node Among all nodes, the aggregator node is selected and monitoring node selection process starts. The MN Select procedure asks for the generation of random numbers for all the neighboring nodes of the Au. Each neighbor sends two random numbers and they are displayed in the node details table. The neighbors are numbered in ascending order and index calculation is made to detect the monitoring node.

Ensuring Secured Transmission A random number is generated and a group key is established to overcome any node compromise attacks. The encrypted data is sent to the destination. The key numbers are referred and entered from the key holder file for confidential transmission. DAA is simulated using MATLAB with 23 random sensor nodes. Simulations are performed for random distribution of sensor nodes. The base station is located at one corner of the network. Simulations are performed using DDAA and Dtradauth equations.

$$D_{\mathrm{DAA}} = (L_{\mathrm{tos}} + 4) \times \left[H + \left(\frac{\beta}{\alpha} \times H_d\right)\right] + \left(1 + \frac{\beta}{\alpha}\right) \times \left[T \times (L_{\mathrm{tos}} + 4) + \frac{4T}{T+1}\right] \text{ bytes} \quad (1)$$

$$D_{\mathrm{tradAuth}} = L_{\mathrm{tos}} \times H \times \left(1 + \frac{\beta}{\alpha}\right) \text{ bytes} \quad (2).$$

Where,
Hd= data aggregator
H=number of hops in random network
Ltos =data packet size
After substituting, H=22 and Ltos=41 in equation 1 and 2, the numerical results are obtained for DDAA and Dtradauth Versus Hd and α/β(false data)

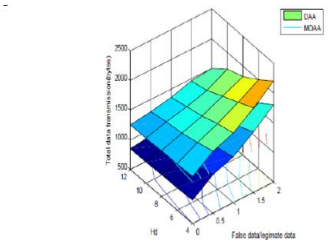

Fig 7: the total transmitted data in DAA is compared to that of the traditional data authentication scheme as the number of data aggregators and the ratio of false data to legitimate data α/β vary

We assume that MDAA is a modified version of DAA such that it is the same as DAA, except that MDAA does not perform any data aggregation at all as shown below in Fig 7. When α/β=2 and the network has 12 data aggregators, DAA results in 60% less data transmission as compared with the traditional data authentication.

This data reduction of up to 60% occurs due to two reasons:

1) The 30% data redundancy is reduced significantly by data aggregation
2) Those false data that could be twice as much as the legitimate data (i.e., α/β could be equal to 2) are detected and dropped as early as possible.

V.CONCLUSION

In this paper has presented the novel security system. The protocol DAA (Data Aggregation and Authentication) detects any false data injected by up to compromised nodes, and that the detected false data are not forwarded beyond the next data aggregator on the path. Thus every sensor node in the network is capable of detecting false data during data aggregation and data forwarding. Our scheme has improved the network security and efficiency during the data transmission in the wireless sensor networks. Despite that false data detection and data confidentiality increase the communication overhead. Data aggregation and authentication are with confidential transit are to be focused with our mechanism DAA and that simulation results show that DAA can still reduce the amount of transmitted data by up to 60% with the help of data aggregation and early detection of false data.

VI. REFERENCES

[1]. C. Intanagonwiwat, D. Estrin, R.Govindan, and J.Heidemann,―Impact of network density on data aggregation in wireless sensor networks, in Proc. b22nd Int. Conf. Distrib. Comput. Syst., Jul. 2002, pp.575– 578.

[2]. Suat Ozdemir, Member, IEEE, and Hasan Çam, Senior Member,―Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks‖ 1063- 6692/$26.00 © 2009 IEEE.

[3]. A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, ―SPINS: Security protocols for sensor networks, Wireless Netw. J., vol. 8, pp.521–534, Sep. 2002.

[4]. C. Karlof, N. Sastry, and D. Wagner, ―TinySec: A link layer security architecture for wireless sensor networks, in Proc. 2nd ACM Conf. Embedded Netw. Sensor Syst., 2004, pp. 162–175.

[5]. C. Blundo,A. Santis, A.Herzberg, S. Kutten, U.Vaccaro, and M.Yung,―Perfectly-secure key distribution for dynamic conferences, in Proc. Crypto, 1992, pp. 471–486.

[6]. P. Gauravaram,W. Millan, J. G. Nieto, and E. Dawson, ―3C—A provably secure pseudorandom function and message authentication code:A new mode of operation for cryptographic hash function, Cryptology ePrint archive, Rep., 2005.

[8] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks," ACM Trans. Sensor Netw., vol. 3, no. 3, Aug. 2007.

[9]. H. Yang and S. Lu, “Commutative cipher based en-route filtering in wireless sensor networks,” in Proc. IEEE VTC, 2004, vol. 2, pp.1223–1227

[10]. D. Seetharam and S. Rhee, “An efficient pseudo random number generator for low-power sensor networks,” in Proc. 29th Annu. IEEE Int.Conf. Local Comput. Netw., 2004, pp. 560–562.

[11]. Suat Ozdemir, Member, IEEE, and Hasan Çam, Senior Member, IEEE, ” Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks”,Vol.18,no.3,June 2010.

[12]. Z. Yu and Y. Guan, “A dynamic en-route scheme for filtering false data in wireless sensor networks,” in Proc. IEEE INFOCOM, Barcelona, Spain, Apr. 23–27, 2006, pp. 1–12.

[13]. R. Rajagopalan and P. K. Varshney, “Data aggregation techniques in sensor networks: A survey,” IEEE Commun. Surveys Tutorials, vol. 8, no. 4, 4th Quarter 2006.

[14]. W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A witness-based approach for data fusion assurance in wireless sensor networks,” in Proc. IEEE GLOBECOM, 2003, pp. 1435–1439.

[15]. I. F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[16]. M. Sivrianosh, D.Westhoff, F. Armknecht, and J. Girao, “Non-manipulable aggregator node election protocols for wireless sensor networks,” in Proc. IEEE WiOpt, Cyprus, Apr. 2007, pp. 1–10.

[17]. F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route detection and filtering of injected false data in sensor networks,” in Proc. IEEE INFOCOM, 2004, vol. 4, pp. 2446–2457.