FALSE DATA DETECTION AND SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

[1]K. Panimalar, [2] M. Priyadharshini, [3]M. Abiya, [4]S. Pushpalatchumy
[1]Assistant Professor, Department of Computer Science Engineering
Sri Manakula Vinayagar Engineering College, Madagadipet, Pondicherry, India
malar.pani123@gmail.com
[2] Final Year, Department of Computer Science Engineering
Sri Manakula Vinayagar Engineering College, Madagadipet, Pondicherry, India
priya.dharshu92@gmail.com
[3]Pre Final Year, Department of Information Technology
Sri Manakula Vinayagar Engineering College, Madagadipet, Pondicherry, India
abiya.fenola6@gmail.com
[4]spush162008@gmail.com

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.*

1. 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 [7]. 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 [7] .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 [1], [2], which enhances the network lifetime because communication constitutes 70% of the total energy consumption of the network [3]. 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. The assumption of the paper is presented in Section II. Section III describes the Data Aggregation and Authentication (DAA) protocol. The simulation results are presented in Section VI. Concluding remarks are made in Section V.

2. LITERATURE SURVEY

2.1 Assumptions

Data aggregation and authentication protocol (DAA) are chosen three limitations. 1) 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. 2) 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. 3) 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 [5]. 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.

2.2 Data Aggregation and Authentication (DAA) Protocol

In this section, DAA provides secure data aggregation, data confidentiality, and false data detection by performing data aggregation at data aggregators. In this work, DAA has to perform three steps as shown flowchart 1.They are

1) 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 in [2].

2) 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.

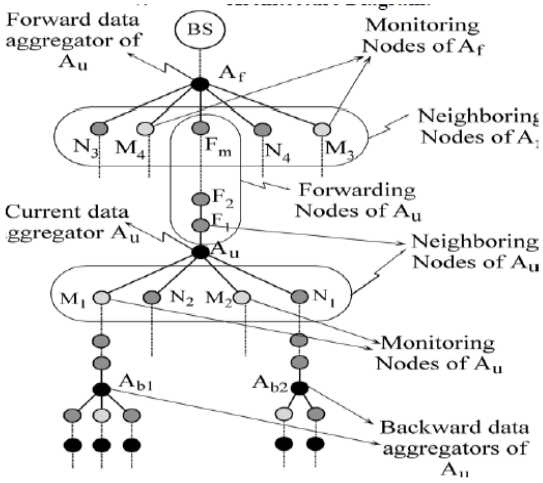

Fig 1 Architecture of DAA

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 $MAC_{K_{f,u}}(N_i$'s) F_j's IDs for $1 \leq j \leq h$
2.	$A_u \Rightarrow T\ M_k$'s	$MAC_{K^u_{group}}(F_1 \mid \cdots \mid F_h)$ for new, random forwarding node labeling $MAC_{K^u_{group}}(N_i$'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

3) 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 verify 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. Each data aggregator forms two FMACs as the following figure 3.

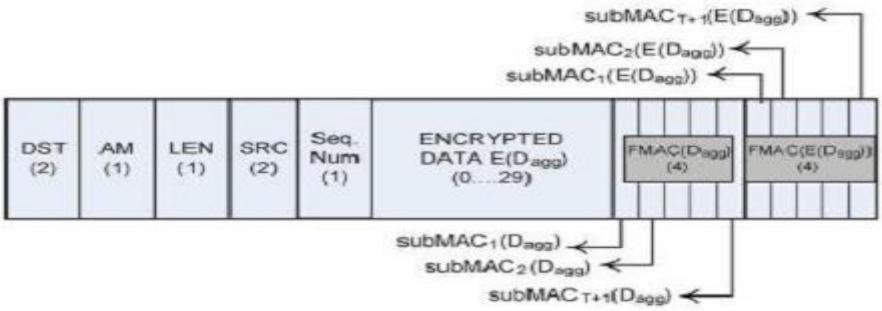

Fig.2: Packet structure of algorithm SDFC

Current data aggregator determines the order of sub Macs and informs each forwarding node about its sub MAC location individually. So, probability of FDI at a forwarding node = (1/2)32.The flowchart for SDFC as shown below in Fig 3.

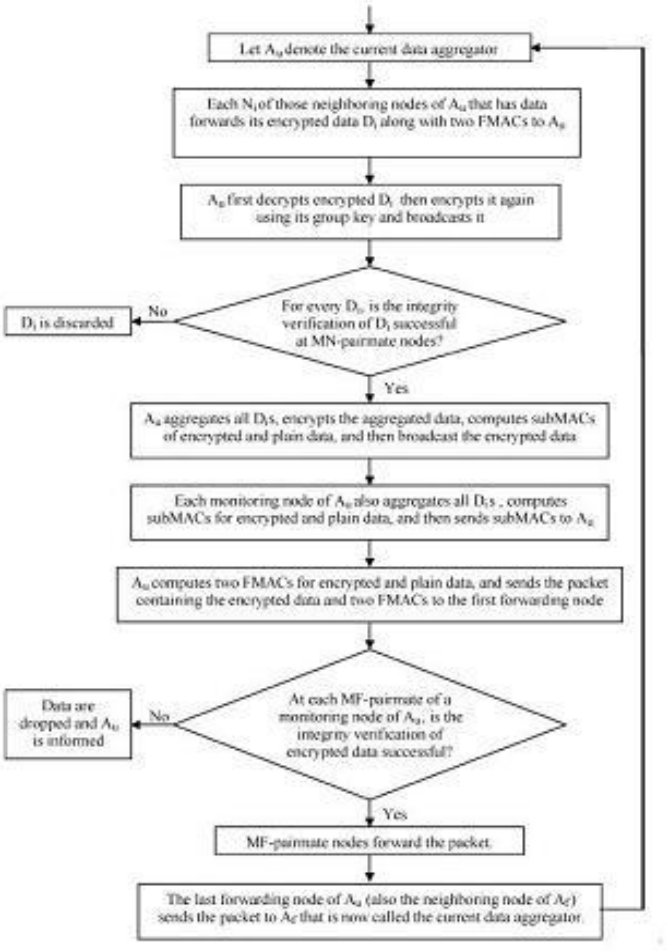

Fig. 3: Flowchart for SDFC

The security of Algorithm SDFC is analyzed with respect to false data detection ability. In Algorithm SDFC, compromised nodes can inject false data during data aggregation or data forwarding. When a sensor node is compromised, the intruder assumed to access all the available security information such cryptographic keys of the node. We present two lemmas to show that Algorithm SDFC can detect any false data injected by up to compromised T nodes. The first lemma shows [2] that Algorithm SDFC detects any false data injected by a compromised data aggregator in the process of data aggregation. To be able to distinguish the injected false data from the aggregated data, the monitoring nodes of every data aggregator also perform data aggregation and compute MACs for the aggregated data. The second lemma shows that Algorithm SDFC can also detect any false data injected by forwarding nodes. The security of a MAC scheme can be quantified in terms of the success probability achievable as a function of total number of queries to forge the MAC [6].

3. SIMULATION RESULTS

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) are shown fig 4,5,6.

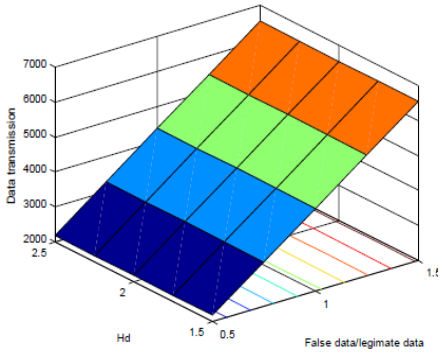

Fig 4: Network with traditional data authentication scheme

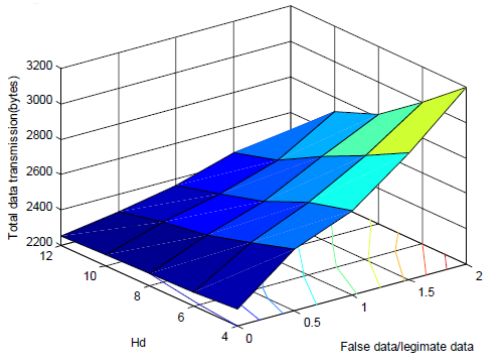

Fig 5: Network with DAA

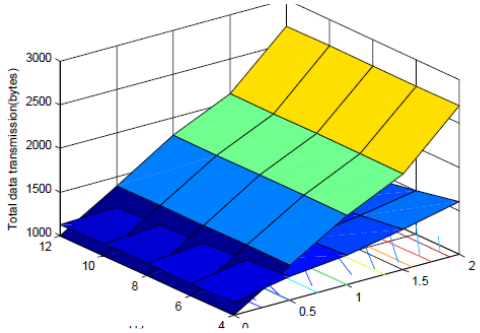

Fig.6: Sensor nodes are random distributed between DAA and tradition data authentication

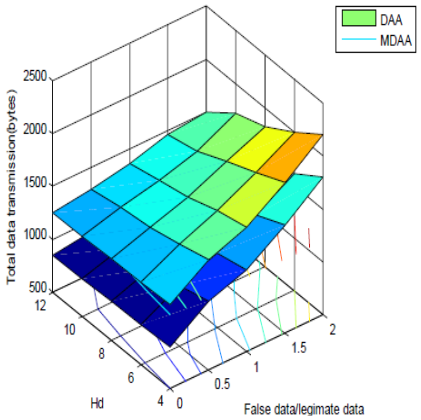

Fig 7: the total transmitted data in DAA is compared to that of the traditional data authentication scheme as the number of data aggregators and the ratio of false data to legitimate data α/β vary

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; and 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.

4. CONCLUSION

In this paper has presented the novel security system. The protocol DAA (Data Aggregation and Authentication) [6] 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.

5. FUTURE WORK

Existing work has provided bounds on lifetime for networks with specific network topologies and source behaviors. It would be interesting to extend this work to more general topologies such as cluster based sensor networks. Another interesting domain of research is the application of source coding theory for data gathering networks. The sensor data are usually highly correlated and energy efficiency can be achieved by joint source coding and data compression. Although some research has been pursued in this direction, there is significant scope for future work

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

Author Profile

K.Panimalar Assistant professor, Department of CSE, Sri Manakula Vinayagar Engineering College, Puducherry. She completed B.Tech (CSE) on 2009 in Sri Manakula Vinayagar Engineering College Puducherry and did M.Tech (CSE) on 2011 in Sri Manakula Vinayagar Engineering College, Puducherry. She presented a paper in 1 National Conference. Her area of interest is Networks.

M. Priyadharshini, Department of CSE, SMVEC, Puducherry. She is pursuing her B.Tech Final year (CSE) in Sri Manakula Vinayagar Engineering College, Puducherry.

M. Abiya, Department of IT, SMVEC, Puducherry. She is pursuing her B.Tech Pre-Final year (IT) in Sri Manakula Vinayagar Engineering College, Puducherry.

S. Pushpalatchumy, worked as Assistant Professor, Department of CSE, Sri Manakula Vinayagar Engineering College, Puducherry. She completed B.Tech (CSE) on 2005 in Rajiv Gandhi College of Engineering and Technology, Puducherry and did M.E (CSE) at 2011 in Dr.Pauls Engineering College, Vilupuram.