International Journal of Smart Sensor and Adhoc Network

Volume 1 | Issue 1 Article 16

July 2011

False Data Detection in Wireless Sensor Network with Secure communication

Priyanka S. Fulare
Department of computer science and engineering G.H. Raisoni College of Engineering and Technology, priyanka1886@gmail.com

Nikita Chavhan
Department of computer science and engineering G.H. Raisoni College of Engineering and Technology, nikichahan@gmail.com

Recommended Citation

S. Fulare, Priyanka and Chavhan, Nikita (2011) "False Data Detection in Wireless Sensor Network with Secure communication," *International Journal of Smart Sensor and Adhoc Network*: Vol. 1 : Iss. 1 , Article 16.
DOI: 10.47893/IJSSAN.2011.1015
Available at: https://www.interscience.in/ijssan/vol1/iss1/16

False Data Detection in Wireless Sensor Network with Secure communication

Priyanka S. Fulare[1], Nikita Chavhan[2]
[1,2]Department of computer science and engineering
G.H. Raisoni College of Engineering and Technology
Email id: priyanka1886@gmail.com[1], nikichahan@gmail.com[2]

Abstract:-The security of wireless sensor networks is a challenging problem in the process of data aggregation. As data are send though sensor network confidentiality plays and important role between sink and destination. An efficient secure data aggregation is proposed to enhance the data security of wireless sensor networks. In wireless sensor networks, compromised sensor nodes can inject false data during both data aggregation and data forwarding. 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. However, In this paper we can see how the data is being remain confidential between sink and destination by using Data authentication method for securing the data in wireless sensor network.

Index Terms-Data aggregation, data integrity, network-level security, sensor networks.

I. INTRODUCTION

WIRELESS sensor networks are vulnerable to many types of security attacks, including false data injection, data forgery, and eavesdropping [1]. Sensor nodes can be compromised by intruders, and the compromised nodes can distort data integrity by injecting useless data. The transmission of useless data depletes the constrained battery power and degrades the bandwidth utilization. Useless data can be injected by compromised sensor nodes in various ways, including data aggregation and relaying. Data aggregation is essential to reduce data redundancy and to improve data accuracy. In addition to useless data detection, data confidentiality is required by many sensor network applications to provide safeguard against eavesdropping.

II. RELATED WORK

1)Efficient Secure in-network Data Aggregation in Wireless Sensor networks:-

The security of wireless sensor networks is a challenging problem in the process of data aggregation. An efficient secure data aggregation is proposed to enhance the data security of wireless sensor networks. Firstly, the secure in-network aggregation tree is introduced, then a judgment method based on trust schema was used to detect whether a sensor node has potential misbehavior. After the detection, a local recovery schema is proposed to reduce the possibility to become isolated nodes, which will increase the security level in data aggregation in wireless sensor networks. The performance analysis shows the efficiency of the schema. The sensor networks we considered is composed of high densely deployed sensor nodes. All the sensor nodes in the networks can be deployed into an hierarchal cluster architecture using some underlying schemes. The clusters are non-overlapping and the cluster head usually perform and aggregation operation on all the reading from the cluster members

belonging to this cluster. Each cluster member can sense the data in the region and can directly communicate with its cluster head to forward its readings results. In some cases, some sensor nodes in this network can be assigned as gateways that can connect all the cluster heads together and transmit their aggregating results to the base station. Sometimes the gateways assigned in the network also have the same sensing capability as other cluster members all received invitation messages.

2)Securing Data Aggregation against False Data Injection in Wireless Sensor Networks

This method proposes a secured data aggregation protocol which detects the false data injection during the data aggregation and identifies the adversary node. The protocol is lightweight because it requires only a minimal cryptographic techniques, and takes *O(n)* time for both data aggregation and tracking back the attacker. Each node shares a unique pairwise key with the base station for authenticated communication between them. Such keys are pre -installed to nodes before the sensor network is deployed.

The proposed solution uses a simple aggregation tree such as a spanning tree constructed by breadth-first search as in ENCAST[9].The sink node floods a discovery message, which is propagated throughout the network. After the flooding, every node knows who are its immediate neighbor nodes and can form a shortest path tree by selecting one of them as its parent. Aggregation tree may be reconstructed periodically, and the base station does not know the topology of the tree (it would be too costly for the base station to learn such information).

The proposed solution requires two kinds of pairwise keys. One is shared between a node and the base station so that the base station can authenticate his message. Such keys are installed before the network is deployed, hence do not require any run-time establishment or management. The other is shared between a node and his parent so that the parent can authenticate his message. Although these keys do require runtime establishment and management, most existing solutions build more expensive cryptosystem on top of them.

3)Statistical En-route Filtering of Injected False Data

In Sensor Networks

Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports. SEF requires that each sensing report be validated by multiple keyed message authentication d e s (MACS), each generated by a node that detects the same event. As the report is forwarded, each node along the way verifies the correctness of the MACS probabilistically and drops those with invalid MACs at earliest points. The sink further filters out remaining false reports that escape the en-route filtering. SEF exploits the network scale to terminal the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes.

In this method we present a Statistical En-route Filtering

Mechanism (SEF). SEF exploits the sheer scale and dense

Deployment of large sensor networks. To prevent any single Compromised node from breaking down the entire system, SEF carefully limits the amount of security information assigned to any single node, and relies on the collective decisions of multiple sensors for false report detection. When a sensing target (henceforth called “stimulus” or “event”) occurs in the field, multiple surrounding sensors collectively generate a legitimate report that carries multiple message authentication codes (MACs). A report with an inadequate number of MACs will not be delivered. As a sensing report is forwarded towards the sink over multiple hops, each forwarding node verifies the correctness of the MACs carried in the report with certain probability. Once an incorrect MAC is detected, the report is dropped. The probability of detecting incorrect MACs increases with the number of hops the report travels. Depending on the path length, there is a non-zero probability that some reports with incorrect MACs may escape en-route filtering and be delivered to the sink. In any case the sink will further verify the correctness of each MAC carried in each report and reject false data.

III PROPOSED PLAN

In the proposed plan, to support data aggregation along with data confidential, 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 pairmates. To support confidential data transmission, the sensor nodes between two consecutive data aggregators verify the data integrity on the encrypted data rather than the plain data. There are T numbers of nodes between two consecutive forwarding nodes or we can say that between two data aggregator. The transmission of false data depletes the constrained battery power and degrades the bandwidth utilization. False data can be injected by compromised sensor nodes in various ways, including data aggregation and relaying. Because data aggregation is essential to reduce data redundancy and/or to improve data accuracy, false data detection is critical to the provision of data integrity and efficient utilization of battery power and bandwidth. In addition to false data

detection, data confidentiality is required by many sensor network applications to provide safeguard against eavesdropping.

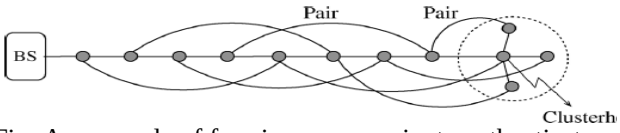

Fig: An example of forming sensor pairs to authenticate data for the false data detection scheme, where data aggregation is not allowed if it requires any change in the data.

Data confidentiality prefers data to be encrypted at the source

node and decrypted at the destination. However, data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation. The existing false data detection algorithms [2]–[5] address neither data aggregation nor confidentiality. Although they could be modified easily to support data confidentiality, it is a challenge for them to support the data aggregation that alters data. For instance, the basic idea behind the false data detection algorithm is to form pairs of sensor nodes such that one pairmate computes a message authentication code (MAC) of forwarded data and the other pairmate later verifies the data using the MAC, as illustrated in Fig. 1. In this scheme, any data change between two pairmates is considered as false data injection, and therefore, data aggregation is not allowed if it requires alterations in the data. Hence, the false data detection algorithm cannot be implemented when a data aggregator between two pairmates changes the data. 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 [6] which enhances the network lifetime because communication constitutes 70% of the total energy consumption of the network [7]. Although data aggregation is very useful, it could cause some security problems because a compromised data aggregator may inject false data during data aggregation. When data aggregation is allowed, the false data detection technique should determine correctly whether any data alteration is due to data aggregation or false data injection. A joint data aggregation and false data detection technique has to ensure that data are altered by data aggregation only. This method introduces a data aggregation and authentication protocol (DAA) to provide false data detection and secure data aggregation against up to T compromised sensor nodes, for T>=1. The value of T depends on security requirements, node density, packet size and the amount of tolerable overhead. We assume that some sensor nodes are selected dynamically as data aggregators, and the nodes between two consecutive data aggregators are called forwarding nodes simply because they forward data. To detect false data injected by a data aggregator while performing data aggregation, some neighboring nodes of the data aggregator (called monitoring nodes) also perform data aggregation and compute MACs for the aggregated data to enable their pairmates to verify the data later. DAA also provides data confidentiality as data are forwarded between data aggregators. To provide data confidentiality during data forwarding between every two consecutive data aggregators, the aggregated data are encrypted at data aggregators, and false data detection is performed over the encrypted data rather than the plain data. Whenever the verification of encrypted data fails at a forwarding node, the data are dropped immediately to minimize the waste of resources such as bandwidth and battery power due to false data injection. The Commutative Cipher based En-route Filtering scheme (CCEF) [4] drops false data en-route without symmetric key sharing. In CCEF, the source node establishes a secret association with base station on a per-session basis, while the intermediate forwarding nodes are equipped with a witness key. With the use of a commutative cipher [8], a forwarding node can use the witness key to verify the authenticity of the reports without knowing the original session key. In the dynamic en-route filtering scheme [5], false data are filtered in a probabilistic nature in the sense that a forwarding node can validate the authenticity of a report only if it has a corresponding authentication key. A legitimate report is endorsed by multiple sensor nodes using their distinct authentication keys from one-way hash chains.

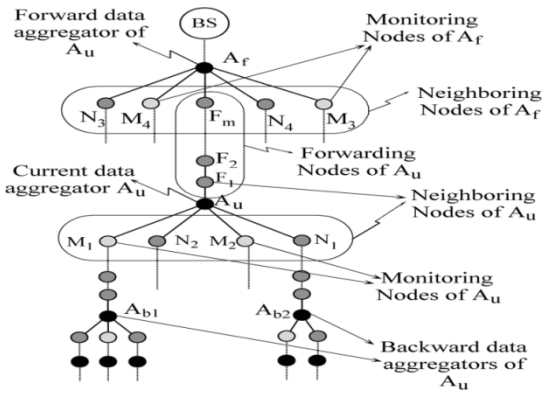

Fig.2 The system architecture of sensor nodes used by DAA. To support false data detection, secure data aggregation, and confidentiality against up to T compromised sensor nodes, DAA forms 2T+1 pairs of sensor nodes by the neighboring and forwarding nodes of Au and Af.

IV. NETWORK MODEL

The main work in network model is selection of data aggregator, secure data aggregator selection protocol (SANE) is used for selection of the data aggregator and data aggregator is selected by taking following condition into account.

1) The data aggregator should have high residual energy.

2) There should be more no. of neighboring node near the data aggregator.

1) Selection of Data Aggregator

The protocol SANE is first run to select candidate data aggregators. Since sector size is determined based on the value of T, the number of intermediate nodes between any two consecutive candidates aggregators is expected to be around. If it happens that there are less than T intermediate nodes between two consecutive candidate aggregators, one of these candidate aggregators drops its candidacy, and then the protocol SANE is run again. This process is repeated until there are at least intermediate nodes between any two consecutive data aggregators.

2) Generation of MAC

In this model only data aggregators are allowed to encrypt and decrypt the aggregated data. The forwarding nodes first verify data integrity using MACs and then relay the data if it is not false.

3) Pairwise key establishment

It is assumed that a monitoring node can establish a pairwise shared key with its pairmate that is multiple hops away. By using random key distribution protocols, monitoring nodes can ensure the identity of their pairmates, thereby preventing Sybil attacks where a compromised node fakes multiple identities to establish pair relations with more than one monitoring node.

4) Limitations

In this subsection, we list the limitations of DAA due to the above assumptions. First of all, the value of T depends strictly on several factors such as geographical area conditions, modes of deployment, transmission range of sensor nodes, power management, and node density of the network.

V. DAA (DATA AGGREGATION AND AUTHENTICATION PROTOCOL)

The DAA(Data aggregator and authentication Protocol) are mainly divided into three group are as follow

1) Monitor node selection (MNS)

2) Forming pairs of sensor node

3) Secure data arrogation and false data detection.

In DAA we have to select Current data aggregator, forward data aggregator and backward data aggregator node

A. Monitor node selection (MNS)

The Monitor node selection for an aggregator to perform secure data aggregation, each data aggregator is monitored by its T neighboring nodes out of total n neighboring nodes, for n>=T. Therefore, in the first step of DAA, T neighbors of data aggregator Au are selected as *monitoring* nodes to perform the data aggregation and to compute subMACs of the aggregated data. The monitoring nodes are selected by the Monitoring Node Selection (MNS) algorithm, as shown in Fig. 4. The basic idea behind the selection of monitoring nodes for each data aggregator in Algorithm MNS is to assign indices to the neighboring nodes in some order and then compute T indices by applying modulus operation to the sum of some random numbers generated by the neighboring nodes. Any neighboring node whose index is equal to one of these T indices becomes a monitoring node. The data aggregator and all neighboring nodes are involved with the selection of monitoring nodes to minimize the adverse impact of a compromised node.

B. Forming Pairs of Sensor Nodes

DAA assumes that a path already exists between any two consecutive data aggregators via forwarding nodes, and that each data aggregator uses only one outgoing path towards base station at a given time. To establish pairs among monitoring nodes and forwarding nodes, Af sends out a “pairmate discovery message” M to Au

to along with its neighboring node list. Af Also adds the MAC of neighboring node list using the key it shares with Au. Message is forwarded by the nodes on the path between Af and Au, and each node that forwards M appends its ID to M . When Au receives M, it has the IDs of its forwarding nodes and neighboring nodes of Af. Let's assume that there are K forwarding nodes (k>=T) between Au and Af . To form the pairs among 's monitoring nodes and forwarding nodes, concatenates the IDs of the forwarding nodes in a random order and indexes them 1 to k . Then, Au computes the MAC of the concatenated IDs and broadcasts the MAC and k.

C. *Integration of Secure Data Aggregation and False Data*

Detection

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 pairs 2T+1 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. subMACs of plain data are used to detect false data injections during data aggregation, whereas subMACs of encrypted data are used to detect false data injections during data forwarding. To detect any false data that the current data aggregator Au can inject *during data aggregation*, the monitoring nodes of also aggregate the incoming data of and compute subMACs for the plain aggregated data, so that the forward data aggregator and its neighboring nodes verify the subMACs. Similarly, to detect those false data that can be injected *during data forwarding*, the monitoring nodes of

compute subMACs for the encrypted aggregated data and then

their pairmates of forwarding nodes verify the subMACs.

CONCLUSION

In the wireless sensor networks, 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, this paper has presented the novel security protocol DAA to integrate data aggregation, confidentiality, and false data detection.

V. REFERENCES

[1] ***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.***

[2] ***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.***

[3] ***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.***

[4] ***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.***

[5] ***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.***

[6] ***C. Intanagonwiwat, D. Estrin, R. Govindan, and J. Heidemann, "Impact of network density on data aggregation in wireless sensor networks," in Proc. 22nd Int. Conf. Distrib. Comput. Syst., Jul. 2002, pp. 575–578.***

[7] ***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.***

[8] ***W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.***

[9] ***L. Hu and D. Evans, "Secure aggregation for wireless networks," in Proc. Workshop Security Assurance Ad hoc Netw., Orlando, FL, Jan. 28, 2003, pp. 384–394.***

[10] ***B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in Proc. SenSys, 2003, pp. 255–265.***

[11] ***D. Wagner, "Resilient aggregation insensor networks." ACM Workshop on Security of Ad Hoc and Sensor Networks, 2004, pp. 78-87.***

[12] ***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.***

[13] ***W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in Proc. 10th ACM CCS, 2003, pp. 42–51.***

[14] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," ACM Trans. Inf. Syst. Security, vol. 8, no. 1, pp.41–77, Feb. 2005.

[15] 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.

[16] S. Xu, "On the security of group communication schemes based on symmetric key cryptosystems," in Proc. ACM Workshop Security Ad hoc Sensor Netw., 2005, pp. 22–31.

[17] "QualNet network simulator," Scalable Network Technologies [Online].Available: www.scalable-networks.com/

[18] 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.

[19] R. L. Rivest, "The RC5 Encryption Algorithm," in Proc. 2nd Int.Workshop FSE, 1994, pp. 86–96.

[20] 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.

[21] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in Proc. 3rd IEEE/ACMIPSN, 2004, pp. 259–268.