Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# The Usage of DAA Protocol in False Data Detection in Wireless Sensor Networks

**P.ANIL KUMAR**
**Asst.Profeesor**
Department of CSE
E-mail: panilkumar6699@gmail.com
MALLAREDDY COLLEGE OF ENGINEERING & TECHNOLOGY, HYDERABAD

**G.DURGA RAMESH**
Pursuing M.Tech
Department of CSE
E-mail: rameshgidugu@gmail.com
MALLAREDDY COLLEGE OF ENGINEERING & TECHNOLOGY, HYDERABAD

***Abstract:*** ***We know that data are travelled from multiple hop in the network during its travelling some are the attacker may inject the false data into the pocket of message. These are cases raised regularly in wireless network because of non reliability[1], of course so many reliable technics are developed by considering that we proposes some methods and protocol called DAA. The 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, this paper presents a data aggregation and authentication protocol, called DAA, to integrate false data detection with data aggregation and confidentiality. 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. 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.***

***Index Terms: —Data aggregation, data integrity, network-level security [1], sensor networks.***

## I .Introduction:

Wireless networks are facing many types of security attacks, including false data injection, data forgery, and eavesdropping[2] . 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[2]. 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[5] 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 Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination [4]. However, data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation

Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission, and improve data accuracy.

## II. Objective of DAA:

This paper has presented the novel security protocol DAA to integrate data aggregation, confidentiality, and false data detection. Data confidentiality[6] prefers data to be encrypted at the source node and decrypted at the destination. 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 in [3] 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.

Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission[7], and improve data accuracy. which enhances the network lifetime because communication constitutes 70% of the total energy consumption of the network. A joint data aggregation and false data detection

 

technique has to ensure that data are altered by data aggregation only. DAA appends two FMACs to each data packet. To reduce the communication

## III. Supporting Systems:

- The existing false data detection techniques [6] consider false data injections during data forwarding only and do not allow any change on the data by data aggregation**.**
- The existing false data detection algorithms[3] address neither data aggregation nor confidentiality.

## IV. Proposed approach:

This paper has presented the novel security protocol DAA to integrate data aggregation, confidentiality, and false data detection [6]. Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination. 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 in is to form

**Approaches of DAA :**

a) Integrating nodes
b) Forwarding data
c) Data integrity
d) Data aggregation detection
e) False data detection

The pairs of sensor nodes such that one pairmate computes a message authentication code (MAC)[8] of forwarded data and the other pairmate later verifies the data using the MAC. Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission, and improve data accuracy. which enhances the network lifetime because communication constitutes 70% of the total energy consumption of the network. A joint data aggregation and false data detection technique has to ensure that data are altered by data aggregation only.

DAA appends two FMACs to each data packet[9]. To reduce the communication. overhead of algorithm SDFC, the size of each FMAC is kept fixed. 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

- DAA also provides data confidentiality as data are forwarded between data aggregators.

### a. Integrating nodes:

A method for integrating wirelessly-communicating network nodes of a process environment into a data communication network by a commissioning facility, comprising: generating a visualization of at least a part of the process environment on an output unit of the commissioning facility as a visualized process environment[4]; detecting a current spatial position of the commissioning facility; showing the commissioning facility in accordance with the current position thereof in the visualized process environment; detecting an identification signal of a network node belonging to the process environment; determining a relative spatial position for the network node in relation to the current spatial position of the commissioning device; generating a proposal for assignment of the identification signal detected, for a node model stored in a database, based on the relative spatial[6] position determined, in relation to the current spatial position of the commissioning device; showing the node model proposed for assignment in the visualized process environment; assigning the network node to the proposed node model by storing address information present in the identification signal of the network node in a variable of the node model proposed for assignment; and showing, after said assigning, a representation of the network node in the visualized process environment.

### b. Forwarding data:

The network layer is responsible for transmitting and routing data packets over the network. The Internet uses the Internet Protocol [8] or IP as its network layer. Each node on the network has an address, which of course is called the IP address. Data is sent as IP packets. A packet has a source, a destination and a payload, and it's passed from one node in the network to another until it gets to the destination.

Each packet can take a different route, and some of the packets may get lost along the way. This response is sent back again in a number of IP packets that will hopefully make it to the client.

### c. Data integrity:

 

The data integrity on the encrypted [9] data rather than the plain data Sensor nodes can be compromised by intruders, and the compromised nodes can distort data integrity by injecting false data.

**d. Data aggregation detection:**

A data aggregation and authentication protocol, called DAA, to integrate false data detection with data aggregation and confidentiality 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 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 data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation[10] Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission, and improve data accuracy hen data aggregation is allowed, the false data detection technique should determine correctly whether any data alteration is due to data aggregation[10] or false data injection. A joint data aggregation and false data detection technique has to ensure that data are altered by data aggregation only.

**e. False data detection:**

Secure Data Aggregation and False Data Detection 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 whereas sub messageauthentication code (MAC) s of encrypted data are used to detect false data injections during data forwarding. To detect any false data that the current data aggregator 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[10] and its neighboring nodes verify the sub MACs. Similarly, to detect those false data that can be injected during data forwarding .

## V. Architecture Diagram:

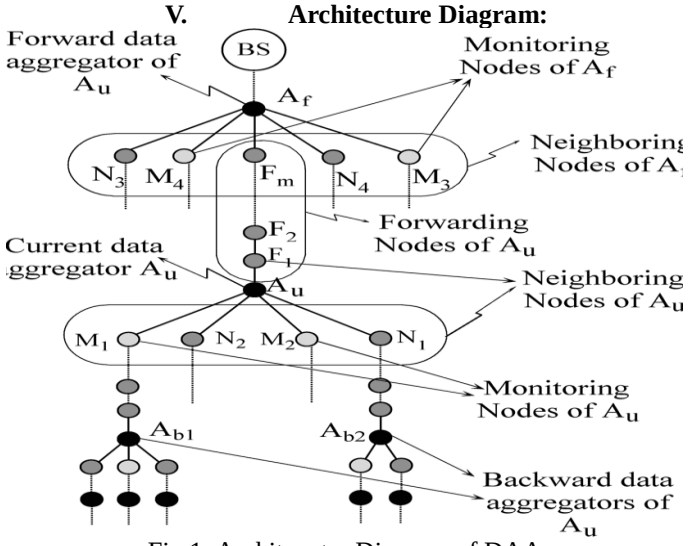


Fig 1: Architecuter Digaram of DAA

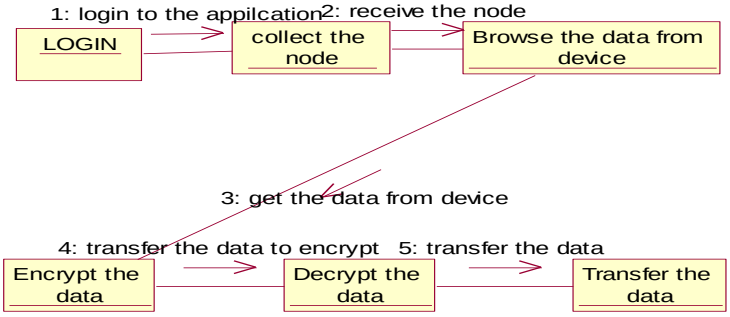


Fig 2: Transmission of data

 

## VI. CONCLUSION

We conclude that the confidential data transmission in sensor nodes between two consecutive data aggregators verify the data integrity on the encrypted data rather than the plain data. The protocol DAA[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. 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.

## REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, 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.

 