Trust based Data Aggregation in Wireless Sensor Networks

Amrutha mohanan.k
PG Scholar, M.E.C.S
Hindusthan College of Engineering and Technology Coimbatore,India

P. Vijayalakshmi
Associate Professor, ECE
Hindusthan College of Engineering and Technology coimbatore,India.

ABSTRACT

The trust based data aggregation scheme is secure and it provides both integrity confidentiality and authenticity for homogeneous and heterogeneous networks and this scheme evaluate the malicious behavior of the nodes. These data aggregation schemes provide better security compared with traditional aggregation since cluster heads can directly aggregate the cipher texts without decryption. In this design an encryption and signature techniques are used and also the base station can recover all sensing data even these data has been aggregated.The base station can perform any aggregation function on them. Without compromising any nodes an attacker can interrupt the network system. The hierarchical trust management protocol detects the malicious behavior of the nodes. It is based on four trust components intimacy, honesty, energy, unselfishness of the nodes. It maintains two levels of trust SN-level trust and CH-level trust

General Terms

Trust evaluation, Encryption, Signature schemes.

Keywords

Data aggregation, Wireless sensor networks, Homogeneous wireless networks, heterogeneous wireless networks.

1. INTRODUCTION

Wireless Sensor Networks (WSN) is the trend of fast few years, and they involve deploying a large number of small nodes. The nodes sense environmental changes and report them to other nodes over flexible network architecture. Sensor nodes are great for deployment in hostile environments or over large geographical areas. Sensors integrated into structures, machinery, and the environment, coupled with the efficient delivery of sensed information, could provide tremendous benefits to society. A WSN typically consists of a sink node sometimes referred to as a Base Station and a number of small wireless sensor_nodes. The base station is assumed to be secure with unlimited available energy while the sensor_nodes are assumed to be unsecured with limited available energy. The sensor nodes monitor a geographical area and collect sensory information. Sensory information is communicated to the Base Station through Wireless hop by hop transmissions. To conserve energy this information is aggregated at intermediate sensor nodes known as cluster head, if whole network divided in to clusters. The aggregation is done by applying a suitable aggregation_function on the received data. Aggregation reduces the amount of network traffic which helps to reduce energy consumption on sensor nodes.

A sensor network should not leak sensor readings to neighboring networks. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality**.** An adversary can easily inject messages, to the WSN so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. The data authentication allows a receiver to verify that the data really was sent by the claimed sender. For providing message authentication we use message authentication code (MAC). MAC is a public function of the message and a secret key that produces a fixed length value that serves as the authenticator.

In communication, data integrity ensures the receiver that the received data is not altered in transit by an adversary. Digital signature schemes are used to provide authenticity and integrity of data. Sender uses a signing algorithm to sign the message. The message and the signatures are sent to the receiver. The receiver receives the message and the signature and applies the verifying algorithm.

Malicious attacks to WSNs can be classified into outsider attacks and insider attacks. The common outsider attacks like spoofing, replay and Sybil attacks can be prevented by cryptography techniques. It is harder to prevent insider attacks. Hierarchical trust management protocol for clustered wireless sensor networks is useful to detect insider attackers

The rest of this paper is organized as follows: Section II deals with the Proposed Scheme, section III discuss with trust management protocol. Section IV comprises security analysis Section V deals with Results and Discussion and Section VI comprises conclusion.

2. METHODOLOGY

The framework for the proposed scheme for homogeneous WSN and heterogeneous WSN are described below.

2.1 Scheme for Homogeneous WSN.

Homogeneous network consist of sensor nodes with same computational capability. This scheme consists of five procedures: Setup, Encrypt-Sign, Trust evaluation, Aggregation, and Verification. The figure 1 shows the sequence of steps involved.

1. Set-up: Base station generates the key pair for each sensor node and base station. The key generation procedure for sensor node is based on Boneh et al's scheme [7]. The keygeneration procedure for base station is based on Mykletun et al's scheme [6]

2. Encrypt-sign: This procedure starts when a sensor node decides to send its sensing data to the clusterhead. This phase consist of three steps. Data is encoded, then signature is produced which is based on Boneh et al's scheme. Then

ciphertext is calculated. It is based on Mykletun et al's scheme. Finally the sensor node sends ciphertext-signature pair to clusterhead.

3. Trust evaluation: In this phase clusterhead evaluate the trust of each sensor node using trust management protocol. Details are given in section 3.

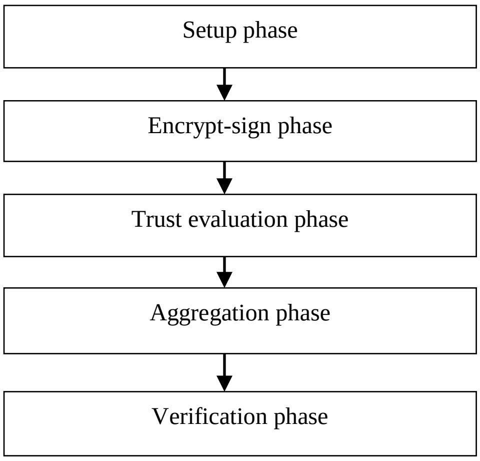

Figure 1 Sequence of steps involved in homogeneous network

4. Aggregation: Here the clusterhead aggregate the ciphertext-signature pair from each sensor node. Aggregation function used is summation of data. Finally the clusterhead sends the aggregated result to the base station.
5. Verification: While receiving ciphertext-signature pair from clusterhead, base station can recover and verify each sensing data. Similarly the base station can receive other ciphertext and signature pairs form other clusters.

2.2 Scheme for Heterogeneous WSN.

Heterogeneous network consist of sensor nodes with different computational capability.It consist of both low value sensor (L-Sensor) and high value sensor (H-Sensor).This scheme consists of six procedures: Setup, Intercluster encrypt, Intracluster encrypt, Trust evaluation, Aggregation, and Verification. The figure 2 shows the sequence of steps involved.
1. Set-up: Base station generates the key pair for each H-sensor and base station. The key generation procedure for H-sensor node is based on Boneh et al's scheme. The key generation procedure for base station is based on Mykletun et al's scheme.
2. Intercluster Encrypt: Each L sensor in the clusterhead shares a pairwise key. In this step L sensor sense the data and encrypt. Finally the ciphertext sends data to the H sensor in the same cluster

3. Intracluster Encrypt: In this stage the H sensor collect all data from the cluster members then it perform the aggregation function. Data is encoded then cipher text is produced by

observations over a time period. Node i can apply overhearing and snooping techniques to detect selfish behaviors of node j

Mykletun et al's scheme. Then signature is produced. It is based on Boneh et al's scheme
4. Trust evaluation: In this phase clusterhead evaluate the trust of each sensor node using trust management protocol. Details are given in section 3.
5. Aggregation: In this step the cluster head aggregate the ciphertext-signature pair from each H sensor. Aggregation function used is summation of data. Finally the clusterhead sends the aggregated result to the base station.
6. Verification: While receiving ciphertext-signature pair from H sensor, base station can recover and verify each sensing data. Similarly the base station can receive other ciphertext and signature pairs form other clusters.

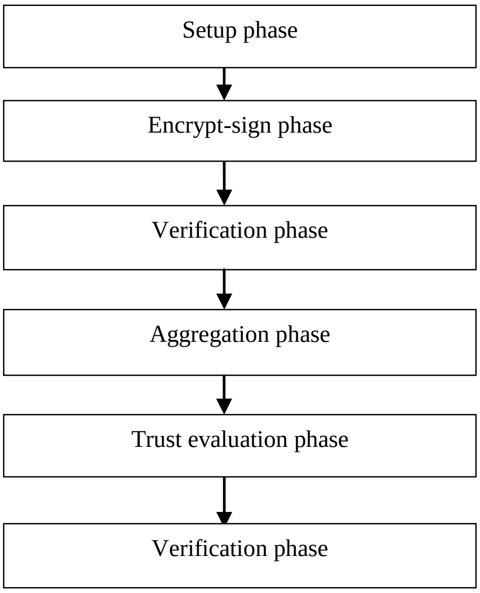

Figure 2 Sequence of steps involved in heterogeneous network.

3. TRUST MANAGEMENT PROTOCOL

The trust management protocol [8] evaluates trust of each sensor node. The evaluation is done by clusterhead.The peer-to-peer trust evaluation is periodically updated based on either direct observations or indirect observations. When two nodes are neighbors within radio range, they evaluate each other based on direct observations via snooping or overhearing.
This trust management protocol is based on four trustcomponents intimacy, honesty, energy, and unselfishness. Intimacy measures the level of interaction between the nodes. If two nodes communicate within certain fixed time period the node is said to satisfy intimacy.
Honesty refers the belief of node i that node j is honest based on node i's direct observations towards node j. Nodei estimates honesty by keeping a count of suspicious dishonest experiences of node j. Dishonest experience can be packet drop.
Energy refers to the belief of node i that node j still has adequate energy to perform its intended function. Node i estimates node j's remaining energy by overhearing node j's packet transmission activities over a time period. Unselfishness of node j is evaluated by node i based on direct such as not faithfully performing sensing and reporting functions, data forwarding functions.

4. SECURITY ANALYSIS

Sensing messages are encrypted to be secured. In Homogeneous network each sensor encrypts their messages before transmitting. In Heterogeneous network, intracluster traffic is encrypted. Besides, our design generates the corresponding signature for each sensing data. Use of trust management protocol helps to aggregate the data using trusted nodes.

5. RESULTS AND DISCUSSIONS

To evaluate the performance of the schemes, execution time is the main measurement of performance evaluation. Without loss of generality, we define processing delay and aggregation delay for deployed sensors. Processing delay indicates the execution time for sensors to produce cipher texts and corresponding signatures. Processing delay is calculated separate for homogeneous network, heterogeneous network and also for trust evaluation.

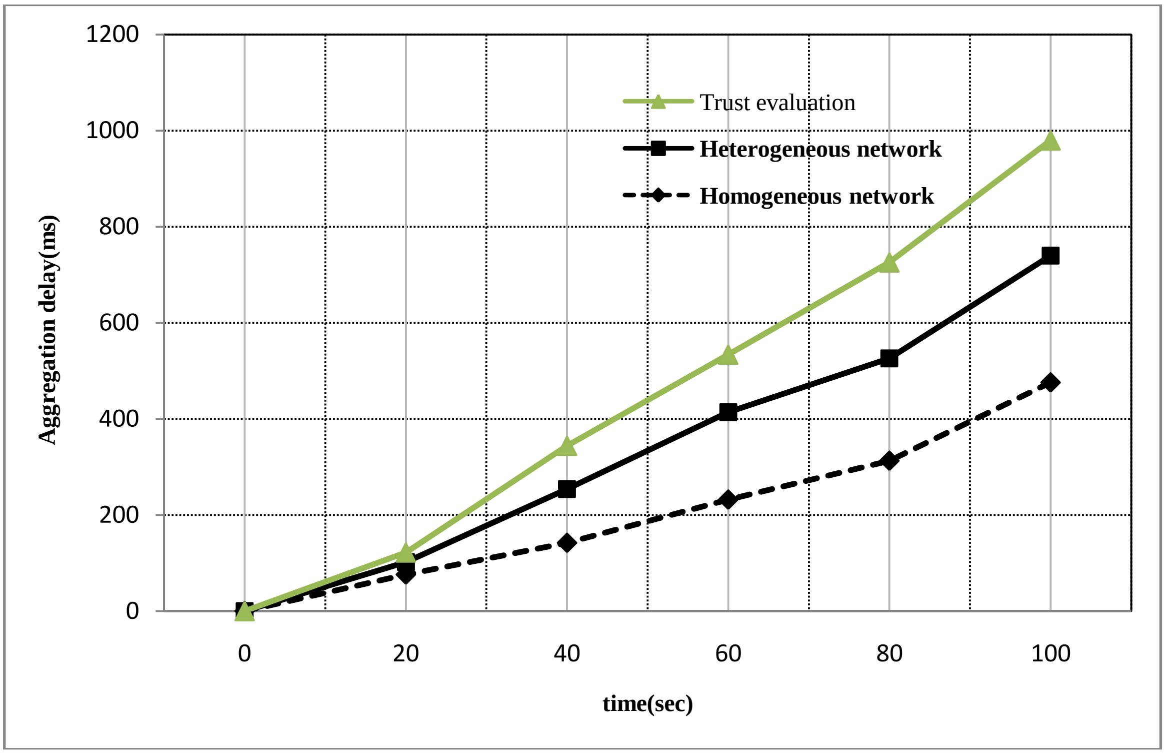

Fig 3: Simulation showing aggregation delay

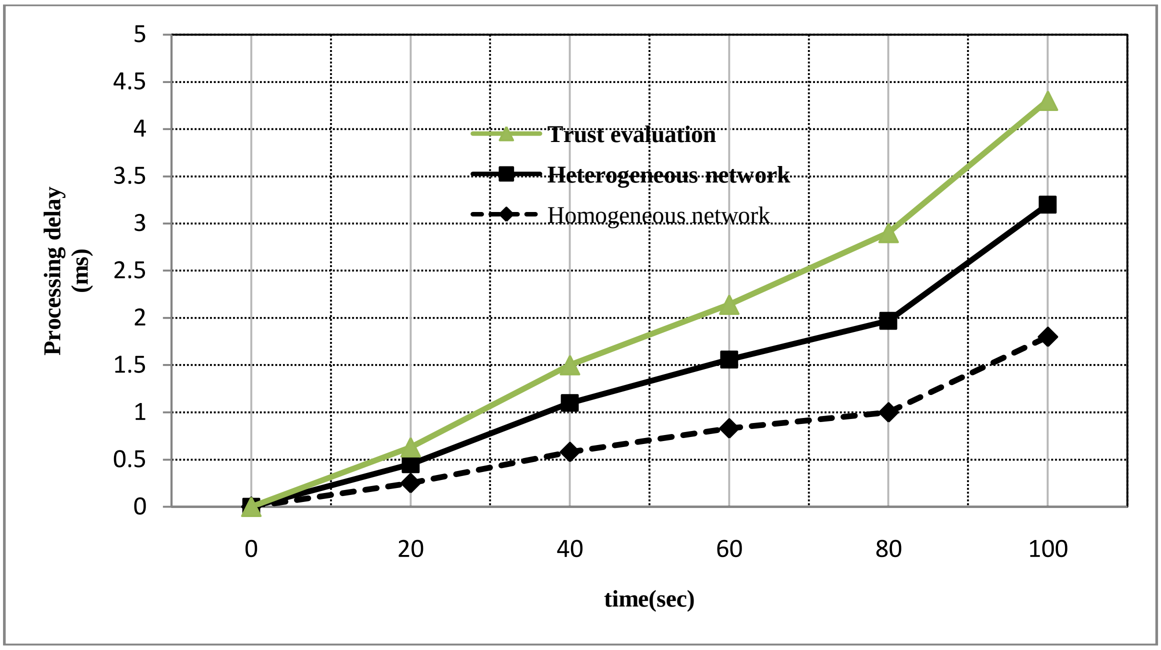

Fig 4: Simulation showing processing delay

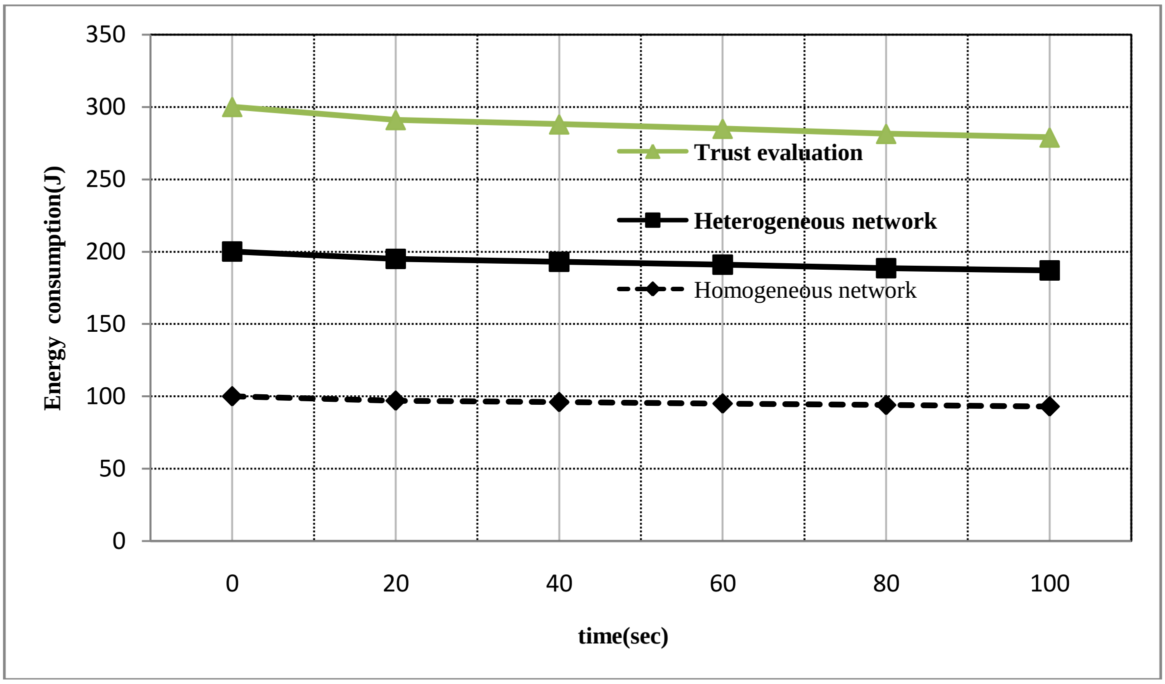

Fig 5: Simulation showing energy consumption

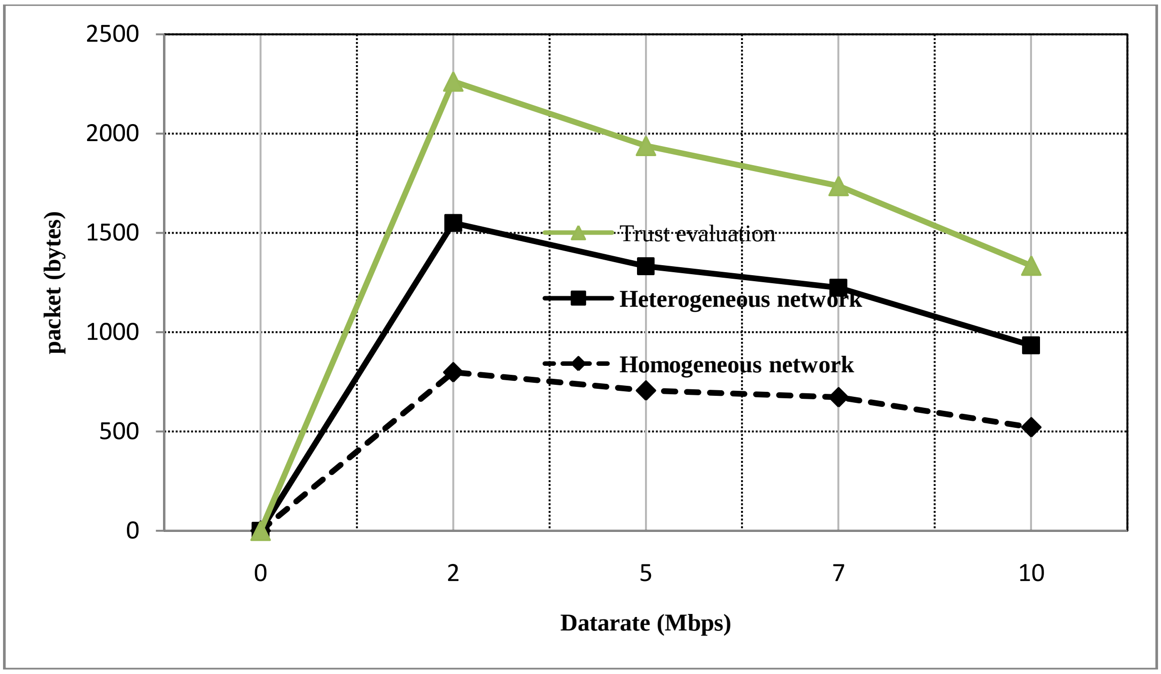

Fig 6: Simulation showing communication cost

6. CONCLUSION

The scheme integrates data aggregation and signature to ensure data authenticity and integrity. The trust management protocol helps to aggregate the data using trusted nodes.

7. ACKNOWLEDGMENTS

Authors would like to thank all the researchers who have contributed in this field of research. The comments of anonymous reviewers to improve the quality of this paper are also acknowledged.

8. REFERENCES

[1] Chien-Ming Chen and Yue-Hsun Lin, 2012 "RCDA: Recoverable Concealed data aggregation for data integrity in wireless sensor networks".IEEE Transactions on parallel and distributed systems, vol.23, no.4.

[2] J.-Y. Chen, G. Pandurangan, and D. Xu, 2006 "Robust Computation of Aggregates in Wireless Sensor Networks: Distributed Randomized Algorithms and Analysis," IEEE Trans. Parallel Distributed Systems, vol. 17, no. 9, pp. 987-1000.

[3] H. Sanli, S. Ozdemir, and H. Cam, 2004 "SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks,"Proc. IEEE 60th Int'l Conf. Vehicular Technology (VTC '04-Fall), vol. 7, pp. 4650-4654.

[4] D. Westhoff, J. Girao, and M. Acharya, 2006 "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor

Networks: Encryption, Key Distribution, and Routing Adaptation," IEEE Trans. Mobile Computing, vol. 5, no. 10, pp. 1417-1431.

[5] C. Castelluccia, E. Mykletun, and G. Tsudik,,2005 "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems, pp. 109-117.

[6] E. Mykletun, J. Girao, and D. Westhoff, 2006 "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm., vol. 5, pp. 2288-2295.

[7] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 416-432, 2003.

[8] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, 2012 " Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust Based Routing and Intrusion Detection," IEEE Transactions On Network And Service Management, Vol. 9, No. 2.

[9] J. H. Cho, A. Swami, and I. R. Chen, 2011 "A survey on trust management for mobile ad hoc networks," IEEE Commun. Surveys Tutorials, vol. 13, no. 4, pp. 562–583.