Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-6, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Secure Data Aggregation with Homographic Primitives hop-by-hop Encryption and end-to-end Encryption

Ms Vaishali S. Gajbhiye[1] & Prof. Pragati Patil[2]
Computer Sci. & Engineering, AGPCET Nagpur

Abstract— *In wireless sensor networks, data aggregation plays an important role in energy conservation of sensors. However, these networks are typically deployed in hostile environments and in which privacy and data integrity are widely desired. Because of their design, wireless sensors can be easily captured. Also, nodes that perform the aggregation function are most attractive to attackers. Therefore, in order to deal with these security threats, the research on data aggregation security is essential. In this context, several solutions have been proposed to secure data aggregation in sensor networks, based on several encryption techniques. Among these, there is the Homographic encryption. Compared to other techniques, in Homographic encryption all the sensor nodes participate in the aggregation, without seeing any intermediate or final result, while still maintaining an effective and efficient aggregation process. We present a survey of some secure data aggregation schemes that use Homographic encryption properties, and then we compared them based on some criteria. Finally, we present and discuss some open issues that need to be looked in future studies in order to improve the security of data aggregation in wireless sensor networks.*

.

Keywords *Wireless sensor networks, Data aggregation Homographic encryption, MAC, Integrity*

A wireless sensor network (WSN) [1] is a set of sensors in a physical environment. These sensors have limited resources in terms of computing, storage, communication, etc. However, the fact that communication is the most costly in terms of energy consumption for a sensor node, a common goal for the applications of WSNs is to reduce the amount of data to be transmitted as much as possible. These data are generally sensor measurements to be collected and routed to a collection point using a multi-hop communication. One possible approach to reduce this amount of data is to use data aggregation [2]. Data aggregation significantly reduces energy consumption and, therefore, is fundamental to many applications of WSNs. The wireless media, however, is inherently dangerous because it is accessible by all users in the transmission range. Also, sensor networks are typically deployed in environments, often very hostile and without assistance (a military application, for example). A certain level of security [3] must be assured. Security requirements concerning data confidentiality (the attacker should not be able to understand the content of the message), data integrity (accidental or malicious changes packets

to be detected), and authentication the receiver should be able to verify that the data are from the supposed source. Unfortunately, data aggregation and security do not go together very well because it should be noted that they have opposite goals. In fact, the first attempts to minimize the amount of data transmitted and the second adds a computational load and non-negligible communication to ensure the verification of some security properties. In summary, the data aggregation protocols must be designed in conjunction with the security protocols, in order to give a good compromise between the complexity of the overall protocol and the level of provided security, and this while maintaining an acceptable energy consumption. Ensure aggregation security is therefore a great challenge. For that, several solutions have been proposed based on multiple encryption techniques. These techniques include Homographic encryption [4], which allows to provide end-to-end privacy and did not need to perform cryptographic operations at intermediate nodes. The main contributions of this paper are listed below: We give a simple background of data aggregation in WSNs. We give a simple overview of Homographic encryption properties. We review the secure data aggregation schemes based on Homographic encryption. We compare and discuss the different schemes based on some criteria, and we provide a statistical analysis to draw several important conclusions. The various schemes we survey, enable us to establish some important research challenges.

The remainder of this paper is organized as follows. Section presents a background of data aggregation in WSNs. In this, we briefly introduces the Homographic encryption. We present an overview of the state of the art for securing data aggregation based on homographic primitives.

Brief Literature Survey

Hu et al . [14] and Przydatek et al . [15] explored the ways to protect the aggregated data in WSNs. Their solutions ensure the protection of sensor readings against outsider adversaries. Although numerous authors claim to provide such hop -by-hop secure data aggregation [9] [16] , they all assume that intermediate nodes are trustworthy. As sensor nodes are deployed in hostile environments, such assumptions may not suit the need of a large number of applications. Therefore, Girao et al . [10] [11] proposed a concealed data aggregation protocol that do not consider trustworthy intermediate nodes. They used Domingo Ferrer 's symmetric key based encryption algorithm [17] to perform encrypted data processing at intermediate nodes. In 2005, Castelluccia et al . [18] [19] proposed a symmetric key based Homographic cryptosystem based on one-time pad. In their cryptosystem, each node is equipped with a unique secret key shared with the base station. Hence, a single compromised node cannot make the whole network vulnerable, as in the case of other symmetric key based techniques [17] [20] . Asymmetric key based Homographic cryptosystems [21] [22] including those based on the elliptic curves [22][23] , are expensive and require more resources compared to their symmetric counterparts [17] [18] [20]. Although concealed data aggregation protects privacy of sensor readings at intermediate nodes, the use of privacy homomorphism [12] makes them inherently malleable [24] . Privacy homomorphism is often being considered as an undesirable property [25] . The algorithms that support privacy homomorphism cannot be secure against adaptive chosen cipher text attack (CCA 2) [26]. Encrypted data processing allows intermediate nodes to aggregate the encrypted sensor readings using publicly available information. Hence, encrypted data processing allows not only genuine aggregator nodes, but it also allows malicious adversaries to process the encrypted data without the need for any secret information. Therefore, the need for an authentication mechanism that ensure the integrity of aggregated data becomes imperative.
Although hop-by-hop integrity verification can be achieved through existing authentication mechanisms, the same mechanisms cannot be used to provide end-to -end integrity verification [27]. The en route aggregation of sensor readings and encrypted data processing make end -to -end integrity verification a formidable challenge.
Agrawal et al . [28] Proposed a Homographic MAC that provides integrity verification in data-centric networks. Homographic MAC aggregates message authentication codes (MACs) to reduce the communication traffic. In addition, Homographic MAC verifies the integrity of aggregated data. Although asymmetric key based Homographic primitives like asymmetric key based Homographic encryption [24] and Homographic digital signature [29] [30] exist in literature, we consider only symmetric key based Homographic primitives due to their relatively fewer resource requirements.

Exiting System

Security research challenges and open questions which may be future research directions to enable secure data aggregation in WSNs. Despite the research efforts to improve this issue, there is no ideal scheme that can meet the security requirements for data aggregation and resolve all the problems caused by the special characteristics of WSNs. Therefore, for WSNs security researchers to focus on the challenges we have set out. Networks are typically deployed in hostile environments and in which privacy and data integrity are widely desired. Because of their design, wireless sensors can be easily captured. Also, nodes that perform the aggregation function are most attractive to attackers. Therefore, in order to deal with these security threats, the research on data aggregation security is essential.

Research Methodology

Eavesdropping: It is the most common and easiest form of attack on data confidentiality. An attacker attempts to obtain private information by overhearing the transmissions over its neighboring wireless links. We assume the attacker can eavesdrop on the entire network. False data injection: This can possibly occur during data aggregation or data forwarding. A compromised node can distort data integrity by injecting false data and then drain the limited energy resources of the network. A joint data aggregation and false data detection technique has to ensure that data are changed by data aggregation only.

• Sybil attack: It is a type of attacks where the attacker is able to present more than one identity within the network. An adversary can launch a Sybil attack and generate *n* or more witness identities to make the base station accept the aggregation results.

Implantation Details

In hop-by-hop encryption, aggregator nodes must decrypt all sensor data they receive, aggregate the data according to the corresponding aggregation function, and encrypt the aggregation result before sending it to next hop node. In end-to-end encryption schemes, one intermediate node receives the cipher texts from leaf nodes and then aggregates them with its own encrypted sensor data; the result will finally be sent to a next node.

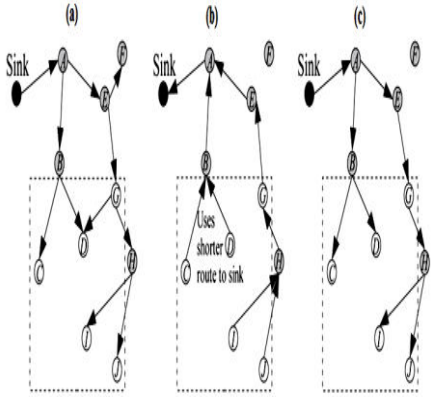

Fig 1. Node Sink

We can classify data aggregation security solutions into two categories namely the hop-by-hop solutions and end-to-end solutions. In the first category, cryptography is applied hop-by-hop, which the security services are checked in each step, the intermediate nodes decrypt each received message and calculate the aggregate before encrypt it. This method allows a simple implementation of aggregate functions, and it imposes no limits on their nature (sum, average, variance, maximum, minimum, etc.) and two types of encryption can be used. Also, these solutions incur significant delay and this is due to the encryption/decryption effort performed by the intermediate nodes. These problems were solved by end-to-end solutions based on a special property of encryption algorithms called privacy Homographic encryption.

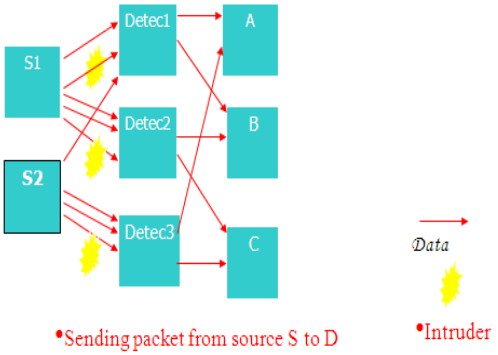

Fig 2. Packet Transmission

The intrusion detection is defined as a mechanism for a PACKET IN NETWORK to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. According port no only we are going to find the path is authorized or Unauthorized.

Conclusion

The standard method to preserve confidentiality is to encrypt the data. Secure data aggregation protocols can be categorized as hop-by-hop encryption and end-to-end encryption. The hop-by-hop secure data aggregation protocols cannot provide data confidentiality at aggregators because the aggregators are required to share keys with their neighboring nodes. In end-to-end secure data aggregation protocols, intermediate nodes aggregate data directly without decrypting the received data. When they are captured, an adversary cannot get the original information. The most common method, named privacy Homographic cryptography, has been studied for data aggregation in WSNs to achieve end-to-end confidentiality

References

[1]. Haythem Hayouni , Secure Data Aggregation with HomographicPrimitives in Wireless Sensor Networks: A Critical Survey and Open Research Issues 2016 IEEE.
[2]. Bhatti, S.; Memon, S.; Jokhio, I.A.; Memon, M.A. Modelling and symmetry reduction of a target-tracking protocol using wireless sensor networks. *IET Commun.* **2012**, *6*, 1205–1211.
[3]. Dyo, V.; , S.A.; Macdonald, D.W.; Markham, A.; Trigoni, N.; Wohlers, R.; Mascolo, C.; Pásztor,

B.; Scellato, S.; Yousef, K. WILDSENSING: Design and deployment of a sustainable sensor network for wildlife monitoring. *ACM Trans. Sensor Netw.* **2012**, *8*, doi:10.1145/2240116.2240118.
[4]. Darwish, A.; Hassanien, A.E. Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors* **2011**, *11*, 5561–5595.
[5]. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. *IEEE Commun. Mag.* **2002**, *40*, 102–114.
[6]. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. *Comput. Netw.* **2008**, *52*, 2292–2330.
[7]. Wang, L.M.; Shi, Y. Patrol detection for replica attacks on wireless sensor networks. *Sensors* **2011**, *11*, 2496–2504.
[8]. Zhu, S.; Setia, S.; Jajodia, S.; Ning, P. Interleaved hop-by-hop authentication against false data injection attacks in sensor networks. *ACM Trans. Sensor Netw.* **2007**, *3*, doi:10.1145/1267060.1267062. *Sensors* **2015**, *15* **15972**
[9]. Ozdemir, S.; Cam, H. Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks. *IEEE/ACM Trans. Netw.* **2010**, *18*, 736–749. 10. Ozdemir, S.; Yang, X. Secure data aggregation in wireless sensor networks: A comprehensiveoverview. *Comput. Netw.* **2009**, *53*, 2022–2037.
[10]. Sang, Y.P.; Shen, H.; Inoguchi, Y.; Tan, Y.; Xiong, N. Secure data aggregation in wireless sensor networks: A survey. In Proceedings of the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), Taipei, China, 4–7 December 2006; pp. 315–320.