e-ISSN: 2349-9745
p-ISSN: 2393-8161

Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

Securing Many-To- Many Wireless Sensor Networks With Unique Dynamic Key

Mrs. Dhanashri D. Dhokate [1], [2], Miss. Ajita A. Patil[3]

Assistant Professor, Information Tech. , PVPIT, Budhgaon, Sangli, INDIA [1]

Associate Professor, Electronics Engg . , PVPIT, Budhgaon, Sangli, INDIA [2]

Assistant Professor, Electronics Engg.. , GCOE, Karad, INDIA [3]

Abstract-Due to the sensitive nature of the data transmitted by applications ranging from mobile target surveillance to intelligent home networking, through Wireless sensor networks, (WSNs) appropriate protection mechanisms are needed to prevent attackers from exploiting the weaknesses of the radio links. In this paper, we propose a novel group key management scheme. This paper investigates the use of secure tunnels as a solution to improve the protection of WSNs. We propose a tunneling scheme that conforms to the security requirements of WSNs while having less computational and network overhead. Our protocol considerably can reduce the number of transmitted messages as well as the computational load, which makes it suitable for WSNs. We tested the proposed protocol considering two models of mobility of the targets which are respectively the Random Walk model and the Gauss Markov model.

Keywords- WSN; cluster security association,Key Distribution Center. Group key exchange.

I. INTRODUCTION

Protocols for authenticated key exchange (AKE) allow parties communicating over an insecure public network to establish a common secret key (a session key) and furthermore to be guaranteed that they are indeed sharing this key with each other (i.e., with their intended partners). Protocols for securely achieving AKE are fundamental to much of modern cryptography and network security. For one, they are crucial for allowing symmetric-key cryptography to be used for encryption/authentication of data among parties who have no alternate \out-of-band" mechanism for agreeing upon a common key. They are also instrumental for constructing \secure channels" on top of which higher-level protocols can be designed, analyzed, and implemented in a modular manner. probabilistic key predistribution scheme for sensor networks is introduced. This solution is based on three steps which are respectively the key predistribution, the determination of the shared key phase, and the path key establishment. In the key predistribution phase, initially a large pool of *P* keys are chosen, and each sensor will be equipped with a key ring stored in its memory. The key ring consisted of randomly chosen keys from the set *P*. Then, the neighboring sensors will find which the common key in their rings is. This key will be used to secure the data sent between the two sensors. This is done in the shared key phase. The last phase is the path key establishment phase. In fact, this solution is probabilistic because it is not guaranteed that all the combination of the pair nodes shares a common key in their randomly chosen rings. Then, a path key has to be assigned for those sensor nodes through two or more links established at the end of the second phase. This solution when compared with the previous solutions necessitates less amount of memory in the sensors because each sensor does not store a key with all the other sensors.

Thus, a detailed understanding of AKE l especially the design of provably-secure protocols for achieving it l is critical. The case of 2-party AKE has been extensively investigated. The progress of sensing and communication technologies has motivated the proliferation of wireless sensor networks (WSNs). Tiny motes [11] connected through radio interfaces can nowadays be implemented for multiple applications including target tracking, virtual reality, and intelligent home networking. The scarcity of the computational, memory, and energy resources, as well as the native vulnerabilities of the radio transmission protocols, increases the need for security services that protect the WSN-based applications. One of the most crucial requirements regarding the security of WSNs is authentication. This stems from the fact that radio links are, by nature, open and vulnerable to various identity spoofing attacks. Moreover, the confidentiality of the gathered data is often an important concern. Secure tunnels have been widely used in traditional wired and wireless networks to guarantee confidentiality and authentication. Unfortunately, the use of traditional tunneling protocols, mainly IPSec and SSL, is not suitable with the specific features of WSNs. Most of the research published in the literature has focused on the development of light cryptographic algorithms that comply with the sensor node capabilities. The objective is to present a solution that permits the authentication of the sensing nodes, formation of ad hoc secure channels for every cluster and security of the exchanges between the nodes. To ensure those we propose a distributed and dynamic tunnel and group key management system for WSNs . We introduce a tunneling approach that takes into account the characteristics of the cryptographic algorithms that are typically used for WSNs.

In this approach there is mi 1-to-1 tunnel but instead of that the Many-to-many(Heterogeneous) tunnel is considered. By this we will ensure several communications between multiple nodes through the same security tunnel. Here a new concept is introduced which is the cluster security association (CSA). The SA is an abstraction of the established many-to-many tunnels and represents shared security attributes between many sensor nodes. The tunnel key is changed periodically so it is a dynamic. Because of this it is very useful for security purpose so that it cannot be used by system after some valid period. The key is not redeployed at the sensors but is dynamically generated. The communicating sensors contribute in a secure manner in this generation. The system provides dynamic integration of new sensor at any time to the global architecture without compromising the security needed.

A new appearing sensor is automatically inserted into the communicating nodes without the need of updates in the other nodes. Then, the system permits all the sensors to exchange directly secured data. This is useful in many applications that necessitate the exchange of data between all the sensors. Military target tracking application needs such communication. When using a group key, each sensor can report its gathered data using the group key to the other sensors. This is advantageous and permits collaboration between the sensors without the need of central node. Firefighting applications. In this case, the sensors are deployed with the firefighter. If all the sensors have the same shared key, any one of the sensors can directly send data to other sensors. Then, the collaboration between the members of the team will be easier by having an efficient dialog between the sensors that represents the firefighter.

II. SYSTEM CONCEPT

The first solutions gives a straight pairwise private key sharing scheme between every pair of nodes. In a deterministic manner, every node shares a key with every other sensor, and the communications are done over 1-to-1 secured tunnels.[5-6] The first problem with that solution is that $n - 1$ keys have to be stored at each sensor node, where n is the number of the nodes in the network. Thus, a large memory space is used to store all the keys. For our solution, only one key is used between a set of sensors that belong to the same group. A compromise of a node will compromise its communication for the entire network, because this sensor node stores in its memory all the network keys. This is not the case solution because the key is always renewed. The other major lack of this solution is that it does not permit a simple group communication. In fact, if a sensor needs to send data to many sensors, it has to do this in many messages. Many copies of the message have to be sent directly to the sensors using the pairwise shared key with each one of the sensors. This is impractical when the number of the sensors belonging to the group becomes larger. For our solution, we have only one key shared with all the sensors. According to this, a node sends the data only one time using the shared group key. Another problem with this solution is the addition of a new sensor to the list of the communicating node. In fact, in those solutions, all the keys are redeployed in the sensors. Then, to add a new sensor, we have to update the keys stored in all the sensors to add the key that will be used with the new sensor. A new sensor can dynamically integrated in a secured communicating group.

Other probabilistic solutions were presented and used for WSNs. Those solutions are qualified as random key distribution solutions. In the basic random key scheme, [5] is introduced. Inspired by this work, additional random key predistribution schemes have been proposed in [1]. The main addition of those works is to increase the resilience of the network against node capture and ensure a smaller need for communication intermediate paths. Those solutions also optimize the required operation time and the number of the stored keys. However, despite all the added techniques, it is always a probabilistic solution. The previous kind of solutions, i.e., those that store a lot amount of keys in the memory of each sensor. This solution does not permit direct group communication between sensors, because the links established are 1-to-1 links. Also, those links are not directly established because its impossible to find a shared key between all the pairs of nodes. Then, if a sensor needs to send data to a group of nodes, it has to do it in a separate manner for each sensor. Another category of the key generation solutions is the centralized key management schemes.

In those schemes, a central node called the key distribution center (KDC) controls and generates the keys used by the sensors. One of the protocol functioning in this manner is the LKHW protocol proposed in [12]. In this scheme, the core node is treated as a KDC, and all keys are logically distributed in a tree rooted at the base station.

The sensors does not contribute in the elaboration of the keys. Then, a compromise of the central node compromises all the network chain. Another lack in this solution is that the keys are distributed in a tree manner. Then, to have a communication between a set of nodes, we do not certainly have a direct secure link between them. Then, a group communication is difficult to be proceeded in these schemes because it will be done as many separate secured connections in a tree communication manner. Having keys distributed in a tree manner does not facilitate the regeneration of the keys and the Integration of a new sensor node in the communicating trusted group of sensors.

A solution that is not a fully centralized solution is also mentioned[12]. The basic idea in PIKE is to use sensor nodes as trusted intermediaries to establish shared keys between nodes. In this solution, they proposed that the key will be established between two sensors through a common trusted third node somewhere within the sensor network. For this solution, initial keys are distributed such as for any two nodes A and B, there is a node C that shares a key with both A and B. Therefore, the key establishment protocol between A and B can be securely routed through C. In this solution, the establishment of the key is secured, and the number of initially deployed keys at the sensor is less than the previous solutions. However, it is not suitable for group communication, because it is least probable that all the nodes of the same group have a common trusted node. The same lacks of the previous categories of solutions are present with this kind of solution.

The LEAP protocol described by Zhu et al. [13] takes an approach that utilizes multiple keying mechanisms. In this scheme, four kinds of messages are established between the different types of sensors:

- An individual key shared with the core node (predistributed).
- A group key that is shared by all the nodes in the network (predistributed).
- Pairwise keys shared with immediate neighboring nodes.
- A cluster key shared with multiple neighboring nodes.

LEAP protocol permits several kinds of communications depending on the needed communicating nodes. This solution provides a many-to-many tunnel protocol like our proposed solution. However, when compared with our solution, it has some lacks:

- The number of the deployed keys at the sensors is large since every pair of sensor nodes needs a key.
- The keys used for several kinds of communication are predeployed into the sensors. This solution uses a static key and does not propose a dynamic generation of the key. For the solution we proposed, the key is renewed after a validity interval.
- In this solution, the keys used for cluster communication are predefined. Then, this solution does not permit a dynamic belonging to the groups. When a sensor needs to change from a group, the key stored in its memory have to be updated and replaced by the cluster key of the new group. That solution is not practical because it needs direct static intervention with each group change. For the proposed solution, the group key is regenerated automatically at periodic times. Then, if a sensor changed from a group, it is automatically integrated in the secured new group when it contributes to the elaboration of the group key.

III. REQUIRED ARCHITECTURE

First emphasize the need for using protected tunnels in the particular context of heterogeneous WSNs. Then, provide a global overview on the distributed security approach. Finally, present the communication exchanges.

Sensor networks can be classified into two categories: simple (or flat) sensor networks and heterogeneous sensor networks. In a flat WSN, all the sensor nodes have the same sensing, communication, and processing characteristics. A heterogeneous WSN integrates various sensor types with different capabilities. The presence of heterogeneous nodes (i.e., nodes with an enhanced energy capacity or communication capability) in a sensor network has the advantage of increasing network reliability and lifetime. Typically, a large number of inexpensive nodes perform simple sensing tasks, while a few expensive nodes (that may be embedded on mobile platforms) provide data filtering, fusion, and transport. This segregation of roles promotes a cost-effective design of the network as well as a more efficient implementation of the overall sensing application. In this paper, the particular case of a heterogeneous WSN is considered which is represented in Figure 1. The network is composed of two layers, the core layer and the sensing layer. The core layer includes nodes which are equipped with powerful sensing and transmission capabilities. Hereinafter, these nodes will be referred to as core nodes. They are able to acquire and exchange voluminous high-resolution data related to the events detected by the low-level sensors. Moreover, this layer constitutes a communication backbone allowing spreading data collected by elementary sensors on a wide area.

The sensing layer consists of miniature devices, also referred to as elementary sensors, whose role is limited to (a) Collecting information about presumably malicious objects, (b) Generating real-time events related to the detected targets and transmitting the events towards the closest core sensor, and (c) Relaying the events generated by other sensors to the core sensors.

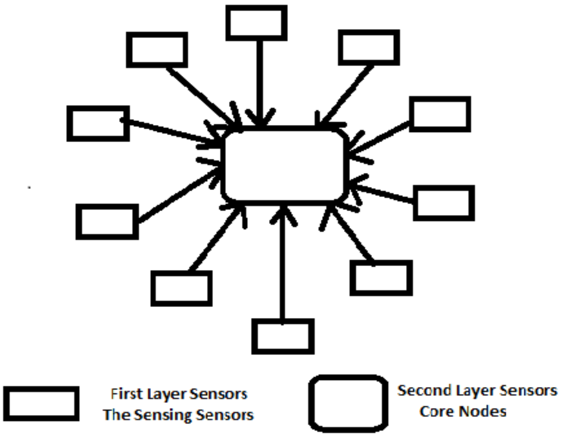

Figure 1: The network architecture.

At the foundation of our approach is the idea of assembling the verification operations of the alert messages originating from multiple sensor nodes to a unique verification step. Based on this reasoning, we define a new requirement called *k*-security [3]. A WSN is called *k*-secure if, and only if, the following properties hold:

1. Every sensor node *si* possesses a private key denoted by *κi*.

2. A unique public key *π* and a subsequent algorithm can be used to verify whether k signatures of the same message generated by distinct sensors are valid or not.

3. An event detected by the sensing layer is considered valid at the core layer if, and only if, k corresponding alert messages are received and successfully verified (as defined in item 2) by the core layer.

The given system share a unique group key between a set of sensors that belongs to the same geographic zone. Then, all the sensors can exchange data between them in a secure and simple manner. Every sensor can send secured data either to the core node or to the other sensors because the group key is known by all the kinds of sensors. The given key generation method includes multiple phases that can be organized according to the context in which the WSN is implemented. To implement this functionality, we consider the group Diffie-Hellman key exchange protocol introduced in [4]. Asymmetric encryption is no longer used because the exchanged tunnel group key is a symmetric key. This is advantageous because the use of the symmetric encryption needs fewer resources than asymmetric encryption. It is then well adapted to the context of the wireless sensor networks. The basic steps of the security scheme are:The core node periodically sends messages to the sensor nodes asking for new information. The sensors that have gathered new information will send reply messages. The core node builds sensor clusters based on the location of the detected events, in the sense that a cluster will include the sensor nodes that have detected the same event. The CSA is set up for every cluster. The tunnel establishment process is authenticated using threshold public key cryptography.

The nodes of the cluster share the same symmetric group key using group Diffie-Hellman key exchange. Many messages will be exchanged between the core node and the sensors. There are two major kinds of messages. The first ones are the messages required to establish the tunnels. The second kind of messages is used to report the events detected by the sensors. The two kinds of messages are sent periodically. We divided the time into slots. At the end of each slot, the sensors send the gathered data to the core node. This reported information is encrypted using the symmetric key shared and established between the core node and all the sensors. The group symmetric key used has a validity interval which is equal to *N* time slots. In this manner, we will not generate a group key in each reporting slot, but we will generate a key used in many time slots. This aims to decrease the time required for the establishment of the keys.

IV. CONCLUSION

In addition to the inputs in terms of security, the system is useful in many applications that necessitate a secure communication among all the nodes such as military target tracking or firefighting collaborating team. The system is with a secure group key and tunneling management protocol for wireless sensor networks. This system aims to establish dynamic secure tunnels between the nodes. To optimize the creation of the tunnels, the protocol creates a shared cluster security association common to the sensor nodes that detect the same event and belongs to the same geographic zone. The system has many advantages. Regarding the security, it permits a dynamic generation of a periodic group key. This shared group key is a symmetric key and then the encryption of the data uses less computational resources than an asymmetric solution. To make our solution dynamic in an architectural term, it can be possible to integrate a newly deployed sensor in the secured set of the sensors.

REFERENCES

1. A Rasheed, R Mahapatra, Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks. IEEE Transactions on Parallel and Distributed Systems (IEEE, Piscataway, 2011), 176–184
2. H Chan, A Perrig, D Song, Random key predistribution schemes for sensor networks. IEEE Symposium on Security and Privacy (IEEE, Piscataway, 2003)
3. M Sliti, M Hamdi, N Boudriga, A Helmy, An elliptic threshold signature framework for k-security in wireless sensor networks. The 15th IEEE International Conference on Electronics, Circuits, and Systems (IEEE, Piscataway, 2008)
4. D Augot, R Bhaskar, V Issarny, D Sacchetti, An efficient group key agreement protocol for ad hoc networks, in *IEEE Workshop on Trust, Security and Privacy in Ubiquitous Computing, WoWMoM 2005,* Taormina, 13–16 June 2005
5. W Du, J Deng, Y Han, P Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, in *Proceedings of the Tenth ACM Conference on Computer and Communications Security (CCS 2003)* (Washington, DC, 27–30 October 2003), pp. 42–51
6. SA Cametepe, B Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks, in *Proceedings of the 9th European Symposium Research Computer Security* (Sophia Antipolis, 13–15 September 2004)
7. L Eschenauer, VD Gligor, A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02) (ACM Press, New York, 2002), 41–47
8. RD Pietro, Mancini LV, Mei A, Random key-assignment for secure wireless sensor networks. Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03) (ACM Press, New York, 2003), 62–71
9. Liu D, Ning P, *Establishing Pairwise Keys in Distributed Sensor Networks*, pp. 52–61
10. W Du, J Deng, YS Han, S Chen, PK Varshney, A key management scheme for wireless sensor networks using deployment knowledge. Proceedings of the IEEE INFOCOM, Hong Kong (IEEE, Piscataway, 2004), 586–97
11. W Bechkit, New key management schemes for resource constrained wireless sensor networks, in *IEEE International Symposium on aWorld of Wireless, Mobile andMultimedia Networks, WoWMoM,* Lucca, 20–24 June 2011
12. M Horton, D Culler, K Pister, J Hill, R Szewczyk, A Woo, MICA, The commercialization of microsensor motes. Sensors. **19**(4), 40–48 (2002).
13. H Chan, A Perrig, PIKE: peer intermediaries for key establishment in sensor networks. IEEE Infocom (IEEE, Piscataway, 2005)
14. S Zhu, S Setia, S Jajodia, LEAP: efficient securitymechanisms for large-scaledistributed sensor networks. 10th ACM Conference on Computer and Communications Security (CCS'03) (ACM Press, New York, 2003), 62–72