www.ioirp.com

International Journal of Innovative Research in Technology, Science & Engineering (IJIRTSE)
ISSN: 2395-5619, Volume – 1, Issue – 3. May 2015

Group Key Management Technique Based On Logic-Key Tree in the Field Of Wireless Sensor Network

[1]Kavitha.P, [2]Prof.Shivamurthy R C
[1]Dept of Computer science & Engg., Akshaya Institute of Technology, Bangalore, India
[2]Prof. & head:Dept. of Computer Science & Engg., Akshaya Institute of Technology, Bangalore, India
[1]kavithaaputhra@gmail.com

***Abstract*— In this recent years the concept of group key management technique is an important issue. Security is a challenging issue in Wireless Sensor Networks (WSNs) due to the dual impact of their inherent constraints and their operation in open and harsh environments. The problem of securing a WSN becomes even more complex when considering group communications. In this paper, we address this problem and propose a new security mechanism for group communications in cluster-tree WSNs. We define a group as a set of sensor nodes in the cluster-tree network sharing the same sensory information (e.g. temperature, pressure, etc.). Our objective is to limit the access to the group data exclusively to the members that have securely joined the group. The main contributions of the paper are the proposal of an efficient and secure group management mechanism for cluster tree networks, and a secure key distribution between group members. Finally, our security analysis shows that the proposed scheme is efficient and secure. However, typical WSNs applications may benefit from being designed and implemented as a collection of multiple logical groups, each one is maintained by a sensor node (the group controller) with constrained resources. In order to go beyond these two limitations, we proposed a new secure group management scheme with a lightweight re-keying process. The scheme allows multiple logical groups, each one is maintained and rekeyed separately by a resource-constrained sensor node without requiring multicast routing support. We proved that the scheme is secure and we evaluated its performance from several view points. Actually, we showed that our scheme outperforms some previous well-known schemes such as LKH.**

Keywords*— *Secure group management, Group communication, Wireless sensor networks (WSNs), Security.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are composed of energy constrained nodes embedding limited transmission, processing and sensing capabilities. Sensor networks have been deployed for a wide variety of applications, including environment monitoring, health-care monitoring, transportation systems, home automation etc. As WSNs are basically deployed in hostile environments, security becomes extremely important, since sensor nodes are exposed to different types of malicious attacks. However, due to resource and computing constraints, security in WSNs imposes several challenges that are more complex than in the other traditional networks. Security in WSNs has attracted several research studies that have addressed various security problems such as authentication [2], [3], key distribution [4], [5], data confidentiality and integrity [6], intrusion detection [7], secure broadcast [8], and Cryptography [9]. The security problem in WSNs becomes even more challenging when dealing with the group security, as this grouping impose additional overhead in terms of network management. Several works have also addressed the latter problem however; each of them relies on a specific and different grouping concept. In this paper, we focus on securing group communications in cluster-tree WSNs, where a group is defined as a set of sensor nodes sharing common private information. This means that sensor nodes in a given group must send and receive messages to/from group members in a way that outsiders are unable to unveil the shared group data, even when they are able to intercept the broadcasted messages.. Thus, the main challenges can be summarized as follows: (1) the initiation and distribution of a group key in a secure and efficient, (2). the management of the group in the cluster-tree network. To illustrate the concept, let us assume that we have a WSN, where some sensor nodes collect temperature data, and other sensor nodes collect humidity data. Thus, we may consider that we have two groups in this particular WSN, and the main motivation is to be able to find adequate solutions to restrict the access to the temperature information to the members of the temperature group, and that of humidity to the members of the other group. Members of humidity group, for instance, should not be able to freely access temperature information without a prior authorization. In other words, grouping is based on the type of data of interest, and this group definition represents one of the contributions of this paper as compared to other related works dealing with secure group communication.

International Journal of Innovative Research in Technology, Science & Engineering (IJIRTSE)
ISSN: 2395-5619, Volume – 1, Issue – 3. May 2015

II. ISSUES IN KEY MANAGEMENT TECHNIQUES

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first

A. Very Limited Resources

Limited Memory and Storage Space A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type (TelosB) has an 16-bit, 8 MHz RISC CPU with only 10KRAM, 48K program memory, and 1024K flash storage [14]. With such a limitation, the software built for the sensor must also be quite small. The total code space of TinyOS, the de-facto standard operating system for wireless sensors, is approximately 4K, and the core scheduler occupies only 178 bytes. Therefore, the code size for the all security related code must also be small.

Power Limitation Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network**.**

B. Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

Unreliable Transfer normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets. This may include, for example, a cryptographic key. Conflicts Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem.

C. Unattended Operation

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes:

Exposure to Physical Attacks the sensor may be deployed I an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network. Managed Remotely Remote management of a sensor network makes it virtually impossible to detect physical tampering (i.e., through tamperproof seals) and physical maintenance issues (e.g., battery replacement). Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed. No Central Management Point A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

D. Security Requirements

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own as discussed in Section 3. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks.

E. Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following:

• A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
• In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
• Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.
The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

F. Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray.
For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment.

G. Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-toned delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. the authors propose a set of secure synchronization protocols for sender-receiver (pair wise), Multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

H. Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data. Adrian Perrig et al. propose a key-chain distribution system for their μTESLA secure broadcast protocol. The basic idea of the μTESLA system is to achieve asymmetric cryptography by delaying the disclosure of the symmetric keys. In this case a sender will broadcast a message generated with a secret key. After a certain period of time, the sender will disclose the

secret key. The receiver is responsible for buffering the packet until the secret key has been disclosed. After disclosure the receiver can authenticate the packet, provided that the packet was received before the key was disclosed

III. RELATED WORK

Group communication security in WSNs is a challenging issue that has been addressed throughout several research works [6 18]. In [6], the authors have proposed SLIMCAST: a secure level key infrastructure for multicast to protect data confidentiality via hop-by-hop re-encryption and mitigate the DoS-based flooding attack through an intrusion detection and deletion mechanism. The SLIMCAST protocol divides a group routing tree into levels and branches in a clustered manner. Communications among nodes in each level of each branch of the group tree are protected by a level key such that only the local level key is updated during a joining or a leaving process. The scheme presents a low communication overhead and power. Consumption and is also scalable. However, the performance is degraded (i.e., high power consumption) when membership changes are massive. In [17], the authors have proposed SeGCom a secure group communications mechanism for cluster-tree wireless sensor networks. The scheme uses lTESLA [19] to broadcast the group controller identity. However, lTESLA requires synchronization of nodes, which is a hard task to achieve in a WSN [20]. Moreover, the scheme did not explain how the authentication process is done and it presents an communication overhead. The authors in [11] have proposed to form a network with multiple base stations, each of which is responsible for dynamically forming a group composed of three types of sensor nodes classified according to their ability to communicate with the base stations. They have also proposed a scheme using a key tree to manage group members as they join or leave the group. However, the authors did not provide details as regards the group rekeying process. As the group key management presents the cornerstone of a secure group communication scheme, several papers have concentrated on the re-keying process. Re-keying occurs whenever a node joins or leaves the group. In LEAP (Localized Encryption and Authentication Protocol) [9], the authors have proposed a key management protocol for sensor networks that are designed to support in-network processing, while at the same time restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node. LEAP supports the establishment of four types of keys for each sensor node—an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a global key shared by all the nodes in the network. For the update of the global key, LEAP assumes the use of a routing protocol in which the nodes are organized into a spanning tree. However, this assumption limits the deployment of the scheme.

Moreover, the scheme rests on the lTesla scheme [19], which requires synchronization between nodes. In [8, 10], the authors have proposed an algorithm to compute a group key in a collaborative manner. The algorithm is based on the multi-party Diffie- Hellman protocol [21]. However, the proposed algorithm requires many exponentially complex operations, which turn it out to be unpractical for sensor networks. In [12–15, 18, 22], the authors have proposed a centralized group rekeying scheme based on a logical key-tree hierarchy for WSNs. The basic scheme is the logical key hierarchy (LKH) [12] proposed to reduce the rekeying messages' number from O(n) to Olog(n), using a tree structure for storing keys. The root of the tree serves as the key distribution center (KDC), while each leaf represents a node. Each leaf stores the set of keys belonging to its direct ancestors up to the KDC. The reason behind applying a tree structure is to increase the re-keying efficiency. However, the energy required for re-keying is approximately logarithmic in the group size. The main contribution of [13] consists of extending the LKH scheme in the context of directed diffusion [23], where the number of rekeying messages is still logarithmic in the group size. Dini et al. [14] have, in turn, improved key authentication by means of key chains, a mechanism derived from Lamport's onetime key and based on hash functions. Furthermore, Dini et al. [15, 22] have later extended the logical key-tree hierarchy into a key graph in order to efficiently support backward and forward security in systems comprising several, possibly overlapping, groups. However, the storage cost required by their scheme exceeds the available resources of a sensor node and, therefore, the scheme cannot be applied to groups with a resource-constrained group controller. The topological key hierarchy (TKH) scheme [18] allows reducing the communication cost of the LKH rekeying messages delivery by mapping the logical key tree to the physical topology. The idea is to construct a key tree that reflects the physical topology of the network. However, TKH does not face with key authentication. In this paper, however, we propose a new secure group communication mechanism based on a logical ring topology, which allows for a scalable re-keying process. The scheme distributes the group management task among group members, thus, eliminating the need for a plentiful group controller. Moreover, the node compromise attack has been addressed, with a proposed solution to detect and discard the compromised nodes.

IV. RESEARCH ISSUES

Although research efforts have been made on cryptography, key management, secure routing, secure data aggregation, and intrusion detection in WSNs, there are still some challenges to be addressed. First, the selection of the appropriate cryptographic methods depends on the processing capability of the sensor nodes, indicating that there is no unified solution for all sensor networks. Instead, the security mechanisms are highly application specific. Second, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. The design of security services in WSNs must satisfy these constraints. Third, most of the current protocols assume that the sensor nodes and the base stations are stationary. However, there may be situations, such as battlefield environments, where the base station and possibly the sensors need to be mobile. The mobility of the sensor nodes has a great influence on sensor network topology and thus raises many issues in secure routing protocols. Some future trends in WSN security research are identified as follows: Exploit the availability of private key operations on sensor nodes: recent studies on public key cryptography have shown that public key operations are still very expensive to realize in sensor nodes. A public key cryptography can greatly ease the design of security in WSNs, improving the efficiency of private key operations on sensor nodes is highly desirable. Secure routing protocols for mobile sensor networks: mobility of sensor nodes has a great influence on sensor network topology and thus on the routing protocols. Mobility can be at the base station, sensor nodes, or both. Current protocols assume the sensor network is stationary. New secure routing protocols for mobile sensor networks need to be developed. Time synchronization issues: current broadcast authentication schemes such as μTESLA and its extensions require the sensor network to be loosely time synchronized. This requirement is often hard to meet and new techniques that do not have such requirement are in demand. Scalability and efficiency in broadcast authentication protocols: new schemes with higher scalability and efficiency need to be developed for authenticated broadcast protocols. The recent progress on public key cryptography may facilitate the design of authenticated broadcast protocols. QoS and security: performance is generally degraded with the addition of security services

V. CONCLUSION

A mutual-healing key distribution scheme using bilinear pairings is proposed in this paper. Security model and formal definition for mutual-healing key distribution were discussed. The proposed new scheme achieves several desirable features. The storage overhead for each node is a constant. The scheme is collusion-free for any coalition of non-authorized nodes. Each authorized node's private key has nothing to do with the number of revoked nodes and can be reused only if it is not disclosed. While in secret sharing-based self-healing key distribution schemes, the personal key can be reused on the condition that less than threshold number nodes are revoked. In addition, their scheme enables a node to recover from a single broadcast message all keys associated with sessions in which it belongs to the session group. The proposed mutual-healing scheme relies on identity and location-based keys. This implies that the proposed scheme can only be used over the wireless networks where nodes are stable. It is not trivial to realize mutual-healing in mobile wireless networks. In fact, the mutual-healing mechanism is more useful in mobile wireless networks because mobile wireless networks have lower network connectivity than stable wireless networks. Therefore, it is significant to investigate new methods to realize the mutual-healing feature in mobile wireless networks.

References

[1] F. Kausar, S. Hussain, J. H. Park, and A. Masood, "*Secure Group Communication with Self-healing and Rekeying in Wireless Sensor Networks*", Springer-Verlag Berlin Heidelberg, pp. 737–748, 2007.

[2] [2]O. Gaddour, A. Koubaa, M. Abid, "*SeGCom: A Secure Group Communication Mechanism in Cluster-Tree Wireless Sensor Networks*", IEEE First International Conference on Communications and Networking, pp.1-7, 2009

[3] M. Garcia, J. Lloret, S. Sendra and R. Lacuesta, "*Secure Communications in Group-based Wireless Sensor Networks*", International Journal of Communication Networks and Information Security, Vol. 2, No. 1, April 2010

[4] B. Tian, S. Han, J. Hub, T. Dillon, "*A mutual-healing key distribution scheme in wireless sensor networks*", Journal of Network and Computer Applications, Elsevier, vol.34, pp.80–88, 2011

[5] O. Cheikhrouhoua, A. Koubaab, G. Dinif, H. Alzaidd, M. Abid, "*LNT: a Logical Neighbor Tree for Secure Group Management in Wireless Sensor Networks*", The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT), ScienceDirect, Elsevier, vol.5, pp.198–207, 2011

[6] O. Cheikhrouhou, A. Koubaa, G. Dini, M. Abid, "*RiSeG: a ring based secure group communication protocol for resource-constrained wireless sensor networks*", Journal Personal and Ubiquitous Computing, ACM Digital Library, vol.15, Iss.8, pp.783-797,2011

[7] H. Nicanfar and V. C.M. Leung, "*Password Authenticated Cluster-Based Group-Key Agreement for Smart Grid Communication", Security* and Communication Networks Security Comm. Networks, pp.1–11, 2012

[8] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "*A Highly Scalable Key Pre-distribution Scheme for Wireless Sensor Networks*", IEEE Transactions on Wireless Communications, vol. 12, Iss. 2, pp.948-959, 2013

[9] S. Bag and B. Roy, "A new key predistribution scheme for general and grid-group deployment of wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, 2013

[10] S. K. Sahoo and M. N. Sahoo, "An Elliptic Curve based Hierarchical Cluster Key Management in Wireless Sensor Network", Springer, 2014

[11] V.K. Singh and K. Sharma, "A Survey on wireless sensor networks security with the integration of clustering and keying techniques", CS & IT-CSCP, pp.183–191, 2013

[12] Q. Siddique, "*Kerberos Authentication in Wireless Sensor Networks*", Computer Science Series. 8th Tome 1st Fasc, 2010

[13] Wang, Xiaoping, Jun Luo, Shanshan Li, Dezun Dong, and Weifang Cheng. "Component based localization in sparse wireless ad hoc and sensor networks." *In Network Protocols, 2008. ICNP 2008. IEEE International Conference on, pp. 288*-297. IEEE, 2008.

[14] Rafaeli, Sandro, and David Hutchison. "*A survey of key management for secure group communication*." ACM Computing Surveys (CSUR) 35, no. 3 (2003): 309-329.

[15] Wong, Chung Kei, Mohamed Gouda, and Simon S. Lam. "Secure group communications using key graphs." Networking, IEEE/ACM Transactions on 8, no. 1 (2000): 16-30.

[16] Lazos, Loukas, and Radha Poovendran. *Secure broadcast in energy-aware wireless sensor networks. Washington* Univ Seattle Dept Of Electrical Engineering, 2002.

[17] Di Pietro, Roberto, Luigi V. Mancini, Yee Wei Law, Sandro Etalle, and Paul Havinga. "LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks." In Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on, pp. 397-406. IEEE, 2003.

[18] Huang, Jyh-How, Jason Buckingham, and Richard Han. "*A level key infrastructure for secure and efficient group communication in wireless sensor network*." In Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on, pp. 249-260. IEEE, 2005.

[19] Perrig, Adrian, Robert Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler. "*SPINS: Security protocols for sensor networks*." Wireless networks 8, no. 5 (2002): 521-534.