Reduced Memory and Communication Overhead in Wireless Sensor Networks using Hybrid Dynamic Key Distribution

Pruthvi P R[1], Shruthi B M[2], Asharani M[3]
[1, 2, 3] Dept. of CSE
[1, 2, 3] GSSSIETW, Mysuru, India

Abstract- *Wireless Sensor Networks are installed in hostile areas. The security issues in wireless sensor networks are very important. Getting secure links between nodes is a challenging problem in WSNs. They are more vulnerable to security attacks than wired networks. In order to protect the sensitive data in WSN can be protected using secret keys to encrypt the exchanged messages between communicating nodes. Key management is essential for many security services such as confidentiality and authentication. The symmetric or asymmetric key cryptography or Trusted-server schemes are used to solve this problem.*

Asymmetric key cryptography increases network security but it increases computational, memory, and energy overhead. Symmetric key cryptography provides less security and it is efficient key management scheme. Trusted server schemes use key management server. Because there is usually no trusted infrastructure it is not very suitable for sensor networks. In this paper, we have proposed Mobile Agent (MA) Based Key Distribution (MAKD). In MAKD, Mobile Agents are used for dissemination of public keys and update of shared keys. Each sensor node constructs different symmetric keys with its neighbors, and communication security is achieved by data encryption and mutual authentication with these keys. Simulation results show that MAKD is scalable and with less memory overhead.

Keywords- Wireless Sensor Networks; Mobile Agents; key management; cryptography

I. INTRODUCTION

Wireless Sensor Network (WSNs) consists of small, low cost and resource limited devices. Their application is to monitor the environment and return the results to the sink node in a single or a multi hop. Each sensor node contains sensing, data processing, memory, and short-range radio communication unit. A sensor has limited computation, storage, bandwidth, and energy resources.

Wireless sensor network applications include target tracking, battlefield surveillance. They are deployed in hostile environments. Therefore the sensitive data should be protected. An adversary can eavesdrop the traffic in a network and eavesdrop the secret messages. Secret keys are used to achieve data confidentiality, integrity. Communicating nodes authenticated and prevent the malicious node impersonating legitimate node for spreading wrong information. An adversary can inject packets, impersonate sensor nodes, provide misleading information and replay older messages. Therefore, security services are crucial. Key management is building block to provide such security services between communicating nodes. Key management is the set of operations which include key generation, setup or distribution, updating, and revocation.

Wireless sensor networks are operated on an unattended mode. An adversary may physically capture sensor nodes to compromise their stored sensitive data and communication keys. Wireless sensors nodes are not tamper resistant due to their low cost. Therefore any adversary can get hold of a sensor node and can easily extract its stored cryptographic information. This attack is defined as node capture attack. Key protection and revocation and updating are considered with special attention in wireless sensor networks. Security solutions are depending very much on the use of strong and efficient key distribution and management. The key management mechanism is responsible for key generation, key distribution, and key maintenance among sensor nodes to establish and maintain secure channels. Key management should also allow sensor networks scaling to a large number of nodes.

A number of key establishment protocols have been proposed over the years. But these methods may not scalable well for large scale sensor networks which are deployed at different locations. Further they may require a large amount of keying information to be pre- loaded into the memory of a sensor. Thus storage space is wasted since much information may never be used during the lifetime of the sensor. They are

also having more communication overhead, computation overhead. They consume more energy. The current key management schemes need more messages transfer in key updating process.

Most of the current key management schemes only suitable for static wireless sensor networks and key management are static. In this paper dynamic key management mechanism for wireless sensor network is proposed. It provides somelevel security for less valuable data. It provides higher levels of security for more sensitive data. Mobile agents are for key distribution and management of the system. This key management mechanism is targeted to reduce the need for storage, communication and computation, and to increase the network lifetime and scalability of the system.

II. RELATED WORK

Considering security, key management is very important. It is very complex in symmetric cryptography structure. Sensor network is dynamic in structure, easy node compromise and self-organized increase the difficulty of key management and bring a broad research issues in this area.

Due to the resource constraints such as energy, memory, processing power, bandwidth and transmission range the distribution and establishment of keys in WSNs is a challenging task. Researchers proposed some approaches to solve those problems, which can be classified into two categories static and dynamic key management schemes. All keys are loaded to the sensor nodes in static approach and each node tries to get the shared keys of the neighbors from the key pool. If a node cannot find a shared key, then it can be set up with the help of one or more intermediate nodes. In dynamic approach some keys are loaded in sensor nodes previously and the session keys can be established by using these keys.

The three keys classify the current proposals as key predistribution schemes, Trusted-server schemes, Self-enforcing schemes based on the main technique that these proposals used or the special structure of WSNs.

- **Key pre-distribution schemes:**

If neighbor node is known in advance deployment, keys can be loaded into sensors. Since in most of applications, sensors are deployed randomly, knowing the set of neighbors deterministically might not be feasible. This type is called probabilistic schemes.

- **Network wide key:**

For secure communication a key called Master or mission key is distributed, to all sensors prior to deployment: any pair of nodes can use this key to achieve key agreement and obtain a new pair wise key. If any node is captured it does not exhibit any network resiliency the entire network security will be compromised.

- **Full Pair wise-keying:**

It lets each node to store N-1 (N, network size, i.e., number of sensors) secret pair wise keys, each is known only to this node and to one of the other N – 1 ones. Because compromising one node does not affect communication of uncompromising nodes the resiliency of the scheme is perfect and it has zero energy cost. Adding new nodes after deployment is difficult because existing nodes do not have the keys of new nodes. It does not suit sensors due to the large amount of memory needed to store the N - 1 keys.

- **Random pair wise keys:**

It is based on a probability distribution (give nodes a certain number of keys) later a node can communicate securely with a neighbor with a given probability p. This probability determines the number of keys given to each node.

B. Trusted-server schemes:

It depends on a trusted third party that is used as key management server. It is not very suitable for sensor networks because there is no trusted infrastructure in WSNs. There is no sensor node that has the capacity to play the role of key server. But this type can be used when the trusted server is an outsider entity connected directly to the WSN. Most of the proposed approaches relied on the base station or sink to be responsible for key management operations.

C. Self-enforcing schemes:

These Schemes depend on asymmetric cryptography such as key agreement using public key certificate. Self-enforcing scheme is not very convenient for WSNs due to high computation overhead.

III. SYESTM ARCHITECTURE

This section discusses the system architecture and its components. The various components of the architecture are presented based on the various agents selected in MAKD are-Public Keys Distribution Agent and Shared Keys update Agent Public Keys Distribution Agent executes the key

distribution algorithm in initial phase. Shared Keys update Agent will update the secret keys.

IV. MAKD

1. Network Model:

MAKD network model has three different kinds of wireless devices; sink node/base station (BS), cluster head node (CH) and sensor node (MN).
Sensor Node (MN): Sensor nodes are limited-capability, generic wireless devices in this paper. Each node has limited battery power, memory size, data processing capability and short radio transmission range.

Cluster head node (CH): Cluster head node has more resources than sensor node. They contain high power batteries, large memory, and powerful antenna and data processing capacities. They can execute complicated numerical operations. CHs can communicate with each other directly and relay data between its cluster members and the base station.

Base station (BS): Sink node has unlimited computational and communication power, unlimited memory storage Capacity, and very large radio transmission range which can reach all the nodes in a network. It can be located either in the center or at a corner of the network based on the application.

2. Threat Model:

The proposed system threat model reflects that the wireless channel is insecure and the communicating nodes cannot be trusted. WSNs are deployed in an unattended, hostile environment. They use insecure wireless channels. The nodes are vulnerable to security attacks and the stored keys can be stolen. These attackers can be classified in two categories. Passive attackers can eavesdrop message exchanges in the network with a compatible radio receiver/transmitter. They will collect and discover valuable information of sensor nodes without disturbing the communication. They do not send any packet into the network. Active attackers inject packets into the networks and can eavesdrop message exchanges. They can interrupt the network communication and overload the traffic. If the attacker gets the secret keys, it can act as if a sensor node and it can communicate with all other nodes within its range. It damages the network functionality by injecting false sensed data. These attacks are called as insider attacks.

V. MAKD

Key Distribution Algorithm

A sensor node can set up a shared key with its neighboring node according to the following key agreement protocol:

Step 1: AV dispatches Mobile Agents.
Step 2: Mobile agents (MA) get the identifier of Source node and the will get the neighbor nodes of node A.
Step 3: Mobile agents (MA) multicast public keys to neighbors and source node.
Step 4: Neighbor nodes use Source node's public key to encrypt a message which contains their identifiers and a random numbers.
Step 5: Source node decrypts the incoming message and obtains the ID and random number of the neighbors. Then it selects a secret key KAB and returns this and Random number which are encrypted using Pubneighbors.

The communicating nodes are verified each other, and they set up a pair wise key which is used to protect communications between these nodes. All transmitted data between these nodes can be protected even if an eavesdropper listens the radio traffic between nodes and tries to inject or modify packets in the network. Secret Keys are periodically updated by using the above algorithm.

VI. RESULTS AND DISCUSSIONS

The proposed MAKD is tested w.r.t. the Memory overhead metric:

Key management mechanism memory usage depends on both the number of nodes. There is only a single key in the network in network wide key mechanism; therefore, it needs minimum memory. In Public key mechanism each node stores public keys of all nodes in the system. When the network size increases, the number of shared keys stored in each sensor node also increases proportional to node count in pair wise key mechanism. Random pair wise key management scheme Memory usage of depends on key ring size of the WSN. The key ring size will be increased with proportional to the number of nodes in the system and key pool size. It increases the probability of neighbor nodes to share at least one key. UAV key management system memory usage of is depends on the number of neighbors. In our proposed system the memory usage further reduced by storing public keys in mobile agents.

The proposed MAKD is tested with respect to the Communication-overhead-metric:

In the proposed architecture, the key sharing will be happening only at the server and cluster node. The further key sharing will take place in the cluster level, thus this will not affect the total network traffic. In WSN, knowledge transmission consumes far more energy than data process. To decrease energy consumption and to extend the network life, it's crucial to decrease the amount and size of the messages.

In each network-wide key theme and pairwise key scheme, shared keys are assigned before readying. In public key scheme, every node stores the general public keys of all nodes within the WSN. Therefore, there's no would like for extra communication between nodes for these schemes. In random pairwise key management mechanisms, there's a requirement of communication for locating shared keys between neighboring nodes as a result of every key ring is generated at random. Within the shared key discovery section, firstly, every node ought to discover its neighbors in its communication range by broadcasting the list of identifiers of the keys on its key ring. In proposed system the communication overhead further reduced by using mobile agents in Cluster head.

VII. CONCLUSION

The design of MAKD is mobile agent based mechanism on large-scale sensor networks with resource constraints. In this scheme, MA executes the algorithm for public keys distribution and keys updating. Only cluster head sensors are in charge of key generation and distribution, which help to conserve resources in normal sensors. A distinctive feature of MAKD is that public keys are distributed by MAs. Simulation study indicates that MAKD has a good performance in terms of key-sharing between neighboring sensors, memory overhead, communication overhead and resilience against node capture.

REFERENCES

[1] O.K. Sahingoz, Multi-level dynamic key management for scalable wireless sensor networks with UAV, in: The Seventh International Conference on Ubiquitous Information Technologies & Applications (CUTE 2012), Ubiquitous Information Technologies and Applications, Lecture Notes in Electrical Engineering, vol. 214, 2013, pp. 11–19.)

[2] K.D. Kim, P.R. Kumar, Cyber-physical systems: a perspective at the centennial,in: Proceedings of the IEEE, vol. 100, 2012, Special Centennial Issue, pp. 1287–1308.

[3] I. Bekmezci, O.K. Sahingoz, S. Temel, Flying ad-hoc networks (FANET): a survey,Ad Hoc Networks 11 (3) (2013) 1254–1270.

[4] M.A. Simplício Jr., P.S. Barreto, C.B. Margi, T.C. Carvalho, A survey on key management mechanisms for distributed Wireless Sensor Networks,Computer Networks 54 (15) (2010) 2591–2612.

[5] J. Zhang, V. Varadharajan, Wireless sensor network key management survey and taxonomy, Journal of Network and Computer Applications 33 (2) (2010)63–75.

[6] X. Chen, K. Makki, K. Yen, N. Pissinou, Sensor network security: a survey, IEEE Communications Surveys & Tutorials 11 (2) (2009) 52–73.

[7] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, M. Galloway, A survey of key management schemes in wireless sensor networks, Computer Communication 30 (11–12) (2007) 2314–2341.

[8] Y. Jeong, S. Lee, Secure key management protocol in the wireless sensor network, Journal of Information Processing Systems 2 (1) (2006) 48–51.

[9] L. Hui, C. Ying, A secure key management protocol for wireless sensor networks, in: 2010 International Conference on Education and Management Technology (ICEMT), 2010, pp. 660–662.

[10] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in: SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy, 2003, pp. 197–213.

[11] E. Munivel, G.M. Ajit, Efficient public key infrastructure implementation in wireless sensor networks, in: International Conference on Wireless Communication and Sensor Computing (ICWCSC 2010), 2010, pp. 1–6.

[12] K. Ren, S. Yu, W. Lou, Y. Zhang, Multi-user broadcast authentication in wireless sensor networks, IEEE Transactions on Vehicular Technology 58 (8) (2009)4554–4564.

[13] A.S. Wander, N. Gura, H. Eberle, V. Gupta, S.C. Shantz, Energy analysis of public-key cryptography for wireless sensor networks, in: Third IEEE International Conference on Pervasive Computing and Communications (PerCom

2005), 2005, pp. 324–328.

[14] D. Gupta, A. De, K. Chatterjee, Performance study of genus 3 hyperelliptic curve cryptosystem, Journal of Information Processing Systems 8 (1) (2012) 145–158.

[15] Sun Microsystems, Inc., Project Sun SPOT: Sun Small Programmable Object Technology (online). <http://www.sunspotworld.com/>, 2013 (accessed 01.01.13).

[16] Certicom, Current Public-Key Cryptographic Systems, A Certicom Whitepaper, 1997, pp. 1–6.

[17] D.E. Boyle, T. Newe, On the implementation and evaluation of an elliptic curve based cryptosystem for Java enabled Wireless Sensor Networks, Sensors and Actuators A: Physical 156 (2) (2009) 394–405.

[18] O.K. Sahingoz, A.C. Sonmez, Agent-based fault tolerant distributedevent system, Computing and Informatics 26 (5) (2007) 489–506.

[19] L. Eschenauer, V.D. Gligor, A key management scheme for distributed sensor networks, in: Proceedings of the Ninth ACM Conference on Computer and Communications Security, 2002, pp. 41–47.

[20] X. He, M. Niedermeier, H. de Meer, Dynamic key management in wireless sensor networks: a survey, Journal of Network and Computer Applications 36 (2) (2013) 611–622.