ISSN:0975-9646

Key Distribution Approaches for Wireless Sensor Networks

Ramu kuchipudi[#1], N Md Jubair Basha[#2]

[#]*IT Department, Muffakham Jah College of Engineering & Technology*
Hyderabad, India

***Abstract*— Wireless sensor networks pose new security and privacy challenges. One of the important challenges is how to bootstrap secure communications among nodes. Several key management schemes have been proposed. However, they either cannot offer strong resilience against node capture attacks, or require too much memory for achieving the desired connectivity. The proposed Bloms algorithm outperforms others in terms of resilience against node capture. Bloms key distribution scheme with deployment knowledge provides a higher connectivity with a shorter transmission range and a lower memory requirement. This paper provides an overview of different approaches of key management schemes and limitations of those approaches.**

***Keywords*—** Key management, Wireless Sensor Networks

I. INTRODUCTION

Wireless sensor networks may consist of a large number of battery-powered sensor nodes, which are equipped with short-range radio, and only have constrained computation capability as well as limited memory space. These sensor networks pose security and privacy challenges when deployed in a hostile environment. For example, an adversary can easily gain access to mission critical or private information by eavesdropping on wireless communications among sensor nodes. Therefore, it is important to encrypt the wireless communication. However, as proposed, the challenge is how to bootstrap [3]secure communications among sensor nodes, that is, how to set up secret keys among sensor nodes to allow them to establish secure links between each other.

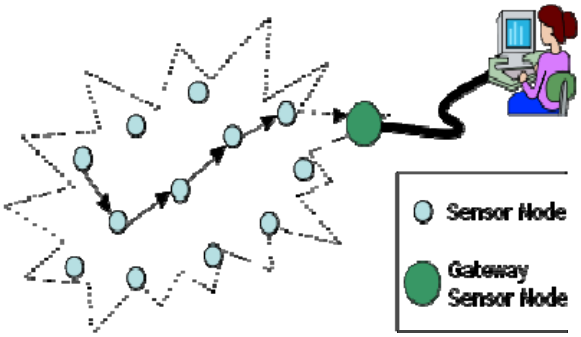

Fig 1.Typical multi-hop wireless sensor network architecture

II. TRADITIONAL KEY MANAGEMENT APPROACHES

Some general key distribution and management approaches are not suitable for wireless sensor networks. First, trivially storing in each node a pair wise key for every other node poses a high memory requirement unaffordable for sensor nodes. Second, online key distribution and management offered by the base station is inefficient for wireless sensor networks due to high communication overhead. Third, public-key algorithms such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) are too expensive to current sensor nodes for high energy consumption and computation overhead. Experimental results from existing research show that the execution time of public key- based operations, such as encryption and decryption, is of the order of seconds or even 10 seconds.

Moreover, wireless sensor networks may not be able to provide the desired public-key infrastructure (PKI) for key distribution. We have to either distribute public keys into nodes through the base station online, which may cause high communication overhead, or pre-distribute public keys into nodes offline, which may need some scheme like what we present in this paper to improve its efficiency.

III. RELATED WORK

A.Drawbacks of Traditional key management approaches

The key agreement problem is a part of the key management problem, which has been widely studied in general network environments. There are three types of general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The trusted-server scheme depends on a trusted server for key agreement between nodes, e.g., Kerberos. This type of scheme is not suitable for sensor networks because there is usually no trusted infrastructure in sensor networks. The self-enforcing scheme depends on asymmetric cryptography, such as key agreement using public key certificates.

However, limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as Diffie-Hellman key agreement or RSA as pointed out. The third type of key agreement scheme is key pre-distribution, where key information is distributed among all sensor nodes prior to deployment.

B.Key Management Scheme for Distributed Networks

Eschenauer and Gligor [6] proposed the basic scheme by predistributing random keys into nodes. The drawback is that one pair wise key may be shared by multiple links.

C.Random Key Predistribution for Sensor Networks

Chan [3] and Perrig presented two schemes. In their q-composite scheme, multiple keys are required to establish a secure link, which makes a trade-off between

connectivity and security. In their random pair wise-key scheme, a unique pair wise key is assigned to each node and every one of a random set. This scheme provides high security but poses an upper bound on network size.

D. Pairwise Key Distribution Scheme for Wireless Sensor Networks

Du[4] proposed the pair wise key predistribution scheme based on both the basic scheme and Blom's scheme, from which it inherits the threshold property.

E. Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks

Du and Liu and Ning[10],[11] independently proposed to utilize deployment knowledge to improve the performance of key establishment. Our scheme outperforms Du's deployment knowledge scheme in terms of connectivity and security. Liu and Ning's polynomial-based key predistribution scheme also has the threshold property for the use of bivariate polynomials, which is a special form of Blom's scheme.

F. A Probabilistic approach for Secure Communication in Wireless Sensor Networks

Zhu[4] presented LEAP by introducing a weaker model, which assumes that there exists a short time interval within which nodes can establish pair wise keys securely. However, this time interval is often very hard to estimate accurately. Once it is overestimated, all links may be compromised.

Probabilistic Key Sharing discussed most of the proposed symmetric key cryptography protocols for establishing a pair wise shared key between two nodes make use of an on-line key server. Mitchell and Piper proposed a solution based on probabilistic key sharing that does not depend on such an on-line server. However, the storage complexity imposed on each participant in their scheme seems to be unaffordable in the context of ad hoc networks.

The probabilistic keying scheme in our protocol is similar to schemes that have been used by other researchers. Eschenauer and Gligor[6] introduced a key management scheme based on probabilistic key sharing for distributed sensor networks (DSN) with central key servers (e.g., base stations).

Chan[3]extended this scheme by presenting three new mechanisms for key establishment in sensor networks based on the framework of probabilistic key predeployment, including a mechanism for pair wise shared key establishment called multipath key reinforcement. Our work differs from the previous ones in several aspects. First, in our scheme, a node can deduce the set of keys it shares with any other node (which may be an empty set) only based on the latter's identity. In contrast, the approaches require each node to exchange the ids of the keys it possesses with its neighbors.

Keys are allocated to each node using a probabilistic scheme that enables every pair of nodes to share one or more keys with certain probability. The keys directly shared between any two nodes can thus be used to encrypt messages exchanged between them. Even if two nodes do not share any keys directly, our probabilistic key sharing scheme enables them to communicate securely using logical paths obtained via a logical path discovery process.

G.Comparision of Different Key Management approaches for Wireless Sensor networks

WSNS are ideal candidates for applications such as military target tracking, home security monitoring, and scientific exploration in dangerous environments. Typically, a sensor network consists of a potentially large number of resource constrained sensors, which are mainly used to collect data (e.g. temperature) from the environment, and a few control nodes, which may have more resources and may be used to control the sensors and/or connect the network to the outside world (e.g. a central data processing server).

Sensors usually communicate with each other through wireless communication channels. Sensor networks may be deployed in hostile environments, especially in military applications. In such situations, the sensors may be captured, and the data/control packets may be intercepted and/or modified.

Therefore, security services such as authentication and encryption are essential to maintain the network operations. However, due to the resource constraints on the sensors, many security mechanisms such as public key cryptography are not feasible in sensor networks. Indeed, providing security services in sensor networks is by no means a trivial problem; it has received a lot of attention recently.

A fundamental security service is the establishment of a symmetric, pairwise key shared between two sensors, which is the basis of other security services such as encryption and authentication. Several key predistribution techniques have been developed recently to address this problem.

Eschenauer and Gligor[6] proposed the basic probabilistic key predistribution, in which each sensor is assigned a random subset of keys from a key pool before the deployment of the network. By doing this, two sensors can have a certain probability to share at least one key. Chan developed the q-composite key predistribution and the random pair wise keys schemes. The q-composite key predistribution scheme is based on the basic probabilistic scheme, but it requires two sensors share at least q predistributed keys to establish a pair wise key.

The random pair wise keys scheme predistributes random pair wise keys between a particular sensor and a random subset of other sensors, and has the property that compromised sensors do not lead to the compromise of pair wise keys shared between non-compromised sensors. However, these approaches still have some limitations.

For the basic probabilistic and the q-composite key predistribution, a small number of compromised sensors may reveal a large fraction of pair wise keys shared between non-compromised sensors. Though the random pair wise keys scheme provides perfect security against node captures, the maximum supported network size is strictly limited by the storage capacity for pair wise keys and the desired probability to share a key between two sensors.

Liu and Ning[9] developed a framework to predistribute pair wise keys using bivariate polynomials and proposed two efficient instantiations, a random subset assignment scheme and a grid-based key predistribution scheme, to establish pair wise keys in sensor networks.

Sensor networks usually consist of a large number of ultra-small autonomous devices. Each device, called a sensor node, is battery powered and equipped with integrated sensors, data processing capabilities, and short-range radio communications. In typical application scenarios, sensor nodes are spread randomly over the deployment region under scrutiny and collect sensor data. Examples of sensor network projects include Smart Dust and WINS.

Sensor networks are being deployed for a wide variety of applications, including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks.

This key agreement problem is a part of the key management problem, which has been widely studied in general network environments. There are three types of general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The trusted-server scheme depends on a trusted server for key agreement between nodes, e.g., Kerberos. This type of scheme is not suitable for sensor networks because there is usually no trusted infrastructure in sensor networks. The self-enforcing scheme depends on asymmetric cryptography, such as key agreement using public key certificates.

However, limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as Diffie-Hellman key agreement or RSA, as pointed out. The third type of key agreement scheme is key pre-distribution, where key information is distributed among all sensor nodes prior to deployment.

If we know which nodes are more likely to stay in the same neighborhood before deployment, keys can be decided a priori. However, because of the randomness of the deployment, knowing the set of neighbors deterministically might not be feasible.

There exist a number of key pre-distribution schemes. A naive solution is to let all the nodes carry a master secret key. Any pair of nodes can use this global master secret key to achieve key agreement and obtain a new pair wise key. This scheme does not exhibit desirable network resilience: if one node is compromised, the security of the entire sensor network will be compromised. Some existing studies suggest storing the master key in tamper-resistant hardware to reduce the risk, but this increases the cost and energy consumption of each sensor.

Based on the Eschenauer-Gligor scheme[6] Chan, Perrig[3] and Song proposed a q-composite random key pre-distribution scheme. The difference between this scheme and the Eschenauer-Gligor scheme is that q common keys (q _ 1), instead of just a single one, are needed to establish secure communications between a pair of nodes. It is shown that, by increasing the value of q, network resilience against node capture is improved, i.e., an attacker has to compromise many more nodes to achieve a high probability of compromised communication.

Du, Deng, Han, and Varshney [5]proposed a new key predistribution scheme, which substantially improves the resilience of the network compared to the existing schemes. This scheme exhibits a nice threshold property: when the number of compromised nodes is less than the threshold, the probability that any nodes other than these compromised nodes are affected is close to zero. This desirable property lowers the initial payoff of smaller scale network breaches to an adversary, and makes it necessary for the adversary to attack a significant proportion of the network. A similar method is also developed by Liu and Ning[9].

A survey on key distribution and authentication for resource-starved devices in mobile environments is given. The majority of these approaches rely on asymmetric cryptography, which is not a feasible solution for sensor networks. Several other methods based on asymmetric cryptography are also proposed: Zhou and Hass propose a secure ad hoc network using secret sharing and threshold cryptography. Kong also proposes localized public-key infrastructure mechanisms, based on secret sharing schemes.

Distributed sensor networks have received a lot of attention recently due to their wide application in military as well as civilian operations. Example applications include target tracking, scientific exploration, and monitoring of nuclear power plants. Sensor nodes are typically low-cost, battery powered, and highly resource constrained, and usually collaborates with each other to accomplish their tasks.

Eschenauer and Gligor[6] proposed a probabilistic key predistribution scheme recently for pair wise key establishment. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment so any two sensor nodes have a certain probability of sharing at least one common key. Chan further extended this idea and developed two key predistribution techniques: q-composite key predistribution and random pair wise keys scheme. The q-composite key predistribution also uses a key pool but requires two sensors compute a pair wise key from at least q predistributed keys they share.

Some general key distribution and management approaches are not suitable for wireless sensor networks. First, trivially storing in each node a pair wise key for every other node poses a high memory requirement unaffordable for sensor nodes.

Second, online key distribution and management offered by the base station is inefficient for wireless sensor networks due to high communication overhead.

Third, public-key algorithms such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) are too expensive to current sensor nodes for high energy consumption and computation overhead. Experimental results from existing research show that the execution time of public key- based operations, such as encryption and decryption, is of the order of seconds or even 10 seconds. Moreover, wireless sensor networks may not be able to provide the desired public-key infrastructure (PKI) for key distribution.

We have to either distribute public keys into nodes through the base station online, which may cause high communication overhead, or predistribute public keys into nodes offline, which may need some scheme like what we present in this project to improve its efficiency

IV. BLOM KEY DISTRIBUTION ALGORITHM

A trusted party gives each participant a secret key and a public identifier, which enables any two participants to independently create a shared key for communicating. Every participant can create a shared key with any other participant, allowing secure communication to take place between any two members of the group. However, if an attacker can compromise the keys of at least k users, he can break the scheme and reconstruct every shared key. Blom's scheme is a form of threshold secret sharing. The scheme was proposed by the Swedish cryptographer Rolf Blom in a series of articles in the early 1980s. Blom's scheme is currently used by the HDCP copy protection scheme to generate shared keys for high-definition content sources and receivers, such as HD DVD players and high-definition televisions.

A. Bloom's Algorithm Steps

1) Choose a random and secret symmetric matrix over the finite field GF(p), where p is a prime number.

2) Choose public identifiers for each of the nodes.

3) Compute private keys by multiplying symmetric matrix and Identifiers of nodes.

4) Exchange identifiers of communicating nodes

5) Compute Shared key by using private key and identifier.

V. CONCLUSIONS

Traditional key management schemes are not suitable for wireless sensor networks. The related work key management approaches are having less computational , space, communication complexities. Some key management schemes are consuming more resources and some are providing less security in the distribution of keys. Bloms key management scheme can be used in wireless sensor networks. In that scheme neighbour nodes can utilize stored secret information more efficiently to generate pair wise keys. It outperforms others in terms of resilience against node capture. Bloms key distribution scheme with deployment knowledge provides a higher connectivity with a shorter transmission range and a lower memory requirement.

ACKNOWLEDGEMENTS

The work was partly supported by the R & D Cell of Muffakham Jah College of Engineering & Technology, Hyderabad, India. The authors would like to thank to all the people from Industry and Academia for their active support.

REFERENCES

[1] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Senso Networks," *Proc. IEEE Symp. Security and Privacy (SP '03)*, pp. 197-213, 2003.

[2] W. Du, J. Deng, Y.S. Han, and P.K. Varshney, "A Pair wise Key Pre-Distribution Scheme for Wireless Sensor Networks," *Proc. 10th ACM Conf. Computer and Comm. Security (CCS '03)*, pp. 42-51, 2003.

[3] W. Du, J. Deng, Y.S. Han, S. Chen, and P.K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," Proc. IEEE INFOCOM, 2004.

[4] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02)*, pp. 41-47, 2002.

[5] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs," *Proc. Sixth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '04)*, pp. 119-132, 2004.

[6] D. Liu and P. Ning, "Establishing Pair wise Keys in Distributed Sensor Networks," *Proc. 10th ACM Conf. Computer and Comm. Security (CCS '03)*, pp. 52-56, 2003.

[7] D. Liu and P. Ning, "Location-Based Pair wise Key Establishment for Static Sensor Networks," Proc. First ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '03), pp. 72-82, 2003.

[8] D. Liu and P. Ning, "Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks," *ACM Trans. Sensor Networks (ToSN*), vol. 1, no. 2, pp. 204-239, 2005.

[9] S. Shakkottai, R. Srikant, and N. Shroff, "Unreliable Sensor Grids: Coverage,Connectivity and Diameter," *Proc. IEEE INFOCOM, 2003.*

[10]] H. Wang and Q. Li, "Efficient Implementation of Public Key Cryptosystems on Mote Sensors," *Proc. Eighth Int'l Conf. Information and Comm. Security (ICICS 06)*, pp. 519-528, 2006.

[11] Z. Yu and Y. Guan, "A Key Pre-Distribution Scheme Using Deployment Knowledge for Wireless Sensor Networks," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), pp. 261-268, 2005.

[12] Z. Yu and Y. Guan, "A Robust Group-Based Key Management Scheme for Wireless Sensor Networks," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), vol. 4, pp. 1915-1920, 2005.

[13] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large- Scale Distributed Sensor Networks," Proc. 10th ACM Conf. Computer and Comm. Security (CCS '03), pp. 62-72, 2003.

[14] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing Pair wise Keys for Secure Communication in Ad Hoc Networks: A Probabilistic Approach," Proc. 11th IEEE Int'l Conf. Network Protocols (ICNP '03), pp. 326-335, 2003.

ABOUT THE AUTHORS

Ramu Kuchipudi received his B.Tech. (CSE) and M.Tech (CSE) from JNTUH, Hyderabad. He is presently working as Assistant Professor in Department of Information Technology, Muffakham Jah College of Engineering and Technology, Hyderabad, India. His research interest includes Computer Networks, Wireless Sensor Networks and MANETS. He is a life member of ISTE. You can reach him at k_ramu2000@yahoo.co.in

N Md Jubair Basha received his B.Tech. (IT) and M.Tech (IT) from JNTUH, Hyderabad. He is presently working as Assistant Professor in Department of Information Technology, Muffakham Jah College of Engineering and Technology, Hyderabad, India. His research interest includes Software Reusability, Network Security and Mobile Computing. He is a active member of IEEE, CSI and CRSI. You can reach him at nawabjubair@gmail.com.