ISSN (e): 2250 – 3005 || Volume, 05 || Issue, 04 || April – 2015 ||
International Journal of Computational Engineering Research (IJCER)

Key Establishment using Selective Repeat Automatic Repeat Request Mechanism for Wireless Sensor Networks

IshwaryaMathi Manickavasagam[1], Madan Mohan Anbalagan[2], InduMathi Manickavasagam[3]
Department of ECE, IT, Tamil Nadu, India

ABSTRACT:
In Key pre-distribution techniques for security provision of Wireless Sensor Networks, a diminutive number of keys are randomly chosen from a large key pool and loaded on the sensors prior to deployment such that they have a common key. Secret keys generated are then placed in sensor nodes, and each sensor node ransacks the area in its communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys, and communication is done on that link between those two nodes. Few neighboring sensors do not share any common key. To establish secure link in such networks, a secret key is exchanged via a multi-hop secure path. But sensors may be compromised on the path rendering process insecure. This paper sets forth a research plan for an enhanced Modified Incremental Redundancy Transmission scheme that uses Selective Repeat Automatic Repeat Request mechanism to address the problem. Through multiple multi-hop paths, the information is transmitted. Only when the destination fails to decode the information, erroneous frame are transmitted to reduce the transmission overhead.

INDEX TERMS—*Wireless sensor networks, key predistribution, randomness, selective repeat*

I. INTRODUCTION

The Wireless sensor network (WSN) is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Secret key establishment is a fundamental requirement for private communication between two entities. Currently, the most common method for establishing a secret key is by using public key cryptography. However, public key cryptography consumes significant amount of computing resources and power which might not be available in certain scenarios. A less expensive and more flexible solution to the problem of sharing secret keys between wireless nodes is to use the inherent randomness in the wireless channel between them as the source for extracting bits of the secret key between these nodes.

Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

II. PROBLEM FORMULATION

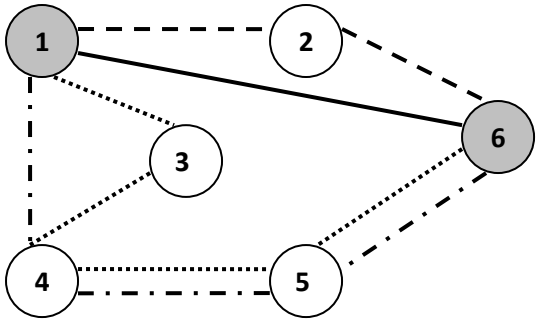


Figure 1: Illustration of path establishment

The key pre-distribution schemes such as [1],[2] and [3] provide memory-efficient and resilient ways of establishing common keys for information transmission for a fraction of potential communication links. The rest of the communication links need to establish their common keys between each pair of nodes by other means such as multihop delivery.

A network topology with few sensor nodes is shown in Figure 1. Each line segment connecting two nodes represents that these two nodes share at least a common key. For example, nodes 1 and 4 share at least a key. Note that nodes 3 and 6 do not share any common key. Now, assume that nodes 1 and 6, as source and destination respectively. They need to establish a secure communication that requires a common key between each pair of nodes in the path established. As suggested in [1],[2] and [3], in order to establish a path with common keys between each pair of nodes between the nodes 1 and 6, a multihop secure path may be used to deliver the message.

The nodes first perform key-discovery to find out with which of their neighbors they share a key. The shared key then becomes the key for that link. After key-setup phase is completed, a connected graph of secure links is formed. If the graph is connected, a path can be found from a source node to its neighbor. For example, we assume nodes 1 and 6 do not share any common keys and therefore the message cannot be transmitted through that path. Node 2 may be used to relay the message between nodes 1 and 6. Since only one multihop path is used, we term it as Single-Path(SP) scheme. Some examples of multihop paths in Figure 1 are 1-6, 1-2-6, 1-4-5-6, 1-3-4-5-6. The dotted line denotes the various paths from the source to the destination node.In general, random key pre-distribution schemes may experience some communication links being exposed when some sensors are compromised. A compromised sensor may modify or drop the secret information passing through the multihop path. This leads to the following problem:

Problem Statement: In key pre-distribution schemes for WSNs, some neighboring sensors do not share any common key. To establish secure link in such networks, multi-hop secure paths are used. However, when any of the sensors on the multi-hop secure path is compromised or captured by the adversary, the part of the information is disclosed. A compromised sensor may also modify or drop the key information passing through itself. What fault-tolerant mechanism should we use to send the information between two physical neighbors efficiently and securely? Note that we work on the problem of sending information between two neighbors that do not share a common key after the key pre-distribution process.

III. BASIC SCHEMES AND MATHEMATICAL MODELS

Key pre-distribution is the method of distribution of keys into nodes before deployment. The network is formed using the secret keys deployed to each node. Key pre-distribution techniques for security provision of Wireless Sensor Networks (WSNs) have attracted significant interests recently.

A key pre-distribution scheme has 3 phases: Key pre-distribution, Shared key discovery, Path-key establishment. In these schemes, a relatively small number of keys are randomly chosen from a large key pool and loaded on the sensors prior to deployment. After being deployed, each sensor tries to find a common key shared by itself and each of its neighbors [1].

Due to the randomness of the key selection process in key pre-distribution, few communication links do not have any common key shared by the two neighboring nodes. Hence a secret link key delivery technique using a multi-hop secure path was proposed: one of the two neighboring nodes finds a multi-hop secure path towards the other node. Each pair of neighboring nodes on the secure path shares at least a common key, which could be different throughout the path.

Such a multi-hop secure path scheme works quite well when all sensor nodes forward the secret key honestly and none of the nodes on the path is compromised. However, the scheme has security problems if any of the nodes is compromised. Such a compromise affects the multi-hop secure path scheme.

In random key pre-distribution, a network need not be fully connected for effective communication to take place. Therefore this technique ensures good connectivity in the network at the same time requires lesser memory space. The EG and Hexagon based deployment model schemes follow random key pre-distribution. [2].

EG Scheme: Eschenauer and Gligor proposed a random key pre-distribution scheme,which is also referred as basic scheme. Let m denote the number of distinct cryptographic keys that can be stored on a node. The basic scheme works as follows. In the initialisation phase a keypool is picked from the key space. Then a set of m key rings are assigned to each node. In the next phase , after the nodes are deployed , the nodes look for shared keys among them and then a link is established upon the discovery of common keys.

Eschenauer and Gligor calculate the necessary expected node degree d in terms of the size of the network n as:

$$d = \left(\frac{n-1}{n}\right)\left(\ln(n) - \ln(-\ln(c))\right) \quad (2.1)$$

For a given density of network deployment, let n be the expected number of neighbors within communication range of a node. Since the expected node degree must be atleast as calculated, the required probability p of successfully performing key-setup with some neighbor is:

$$p = \frac{d}{n'} \quad (2.2)$$

Improving Key predistribution Using Hexagon Based Deployment Model: The centre of a grid is a deployment point, which is the desired location of a group of nodes. The location of node over the entire node field follows some distribution with a probability density function. In hexagon-based scheme, all adjacent sensor nodes have the same distance.

In the hexagon system, first, when a node transmits data over wireless links, its signal range would form a circle that is centered around its deployment location with the radius being the distance of signal propagation. Therefore, a hexagon can be used to express and simulate the signal range more approximately. Second, a hexagon can be used to describe equal distance between two neighboring nodes. Under the hexagonal coordinate system, all adjacent sensor nodes have the same distance which is normally 1 unit.

If the number of nodes is too large, we may divide them into groups and deploy one group each time. Each group of nodes may be deployed into a local area or to just a single deployment point, which is the desired location of nodes. In a group-based deployment model, there are two generally used distributions: In most cases, nodes are often assumed to be uniformly deployed i.e. Uniform distribution. The actual model for the deployment distribution depends on the deployment method.

In the hexagon-based scheme, each nodes center is its deployment hexagon. It shares keys with the nodes deployed in its 19 adjacent hexagons. In Figure.2 all nodes deployed in shaded hexagon can share key with the sensor nodes deployed in hexagon 5. The hexagon based pre-distribution scheme has three phases.

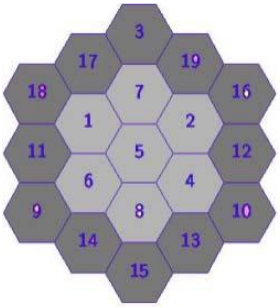


Figure 2: Hexagon co-ordinate system

Proposed scheme: Typically, data transmission is not strictly delay-sensitive but requires a virtually error-free link. To provide reliability over wireless channels, in this work we analyze the modified Incremental Redundancy Transmission scheme,i.e., IRT scheme based on the Selective Repeat protocol allowing transmission of packets without waiting for acknowledgement. In this ARQ, the sender and receiver window size must be equal, and half the maximum sequence number to avoid miscommunication.

Selective Repeat ARQ protocol may be used as a protocol for the delivery and acknowledgement of message units, or it may be used as a protocol for the delivery of subdivided message sub-units.

In this work, we propose a key pre-distribution scheme which improves the resilience of the network with decrease in the fraction of nodes compromised compared to previous schemes and supports flexibility in terms of connectivity. The proposed scheme also enhances the average rate of successful message delivery over a communication channel.

Initially, after the deployment of keys to each node the network is formed. Path is established from the source to the destination between nodes with common keys and the corresponding hop count of each path is obtained.

When Selective Repeat ARQ is used as a protocol for the delivery of messages, even after a frame loss, the sender continues to send frames specified by a window size. Unlike Go-Back-N ARQ, the receiver will continue to accept and acknowledge frames sent after an initial error.

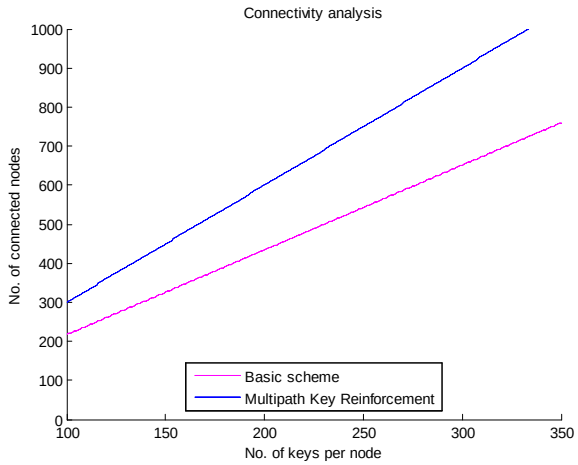
The receiver keeps track of the sequence number of the last frame it has not received. Even if the receiver does not receive a frame, the ender keeps sending subsequent frames until it has sent all the frames in the window. The receiver accepts the subsequent frames and replies with an acknowledgement containing the sequence number of the last missing frame. After all the frames in the window are sent, the sender re-sends the frame number given by the ACKs, and then proceeds where it left off.

Selective Repeat ARQ is used as a protocol for delivery of subdivided messages, where messages are variable in length. For this selective retransmission may be employed in conjunction with the basic ARQ mechanism.

The original variable length message is a concatenation of a variable number of sub-blocks. The message is first subdivided into sub-blocks based on hop count of the established paths, in a process called packet segmentation. The number of frames transmitted is based on the window size. In ARQ with selective transmission the negatively acknowledged response would carry a bit flag indicating the identity of each sub-block successfully received. If the received frame is erroneous, it is rejected and selectively re-transmitted. When frame is received successfully it is acknowledged. Selective re-transmission applied to variable length messages completely eliminates the difficulty in delivering longer messages, as successfully received sub-blocks are retained after each transmission and outstanding sub-blocks in following transmissions diminishes.

IV. PERFORMANCE EVALUATION

Simulations have been performed in Matlab to evaluate the efficiency of the proposed scheme. We investigate the performance of the modified IRT scheme and other related schemes. These schemes include the Incremental Redundancy Transmission scheme, the SP scheme, Hexagonal based deployment model scheme and the random key pre-distribution scheme.



Path Availabilities: In Figure 3, we show the number of paths with secure connections that are exactly h hops from a source to a destination (assuming that they do not share a common key). The average number of paths is presented, corresponding to various local connectivity. We also present the number of paths for a similar network with half the nodes for comparison purposes. As shown in Figure 3, the number of available paths increases with the local connectivity. When the node density increases, there are more paths as well. The number of h-hop paths also increases with h. Note that these paths may have common nodes other than the source and the destination.

Transmission Overhead: When there are compromised nodes on the paths used to deliver the information and these compromised nodes modify the passing information, extra symbols need to be transmitted. The SP scheme randomly chooses one out of the available paths to send the information.

The sender sends a number of frames specified by a window size even without the need to wait for individual ACK from the receiver. The receiver accepts out-of-order frames and buffers them. The sender individually retransmits frames that have timed out and erroneous frames. To reduce the total information that needs to be transmitted, the redundant symbols are transmitted only if the destination fails to decode the information successfully. Therefore reducing the transmission overhead and increasing the performance efficiency.

Security Analysis: The fraction of total keys being compromised can be expressed as,

$$p = 1 - \left(1 - \frac{m}{|s|}\right)^{x} \qquad 4.1$$

The equation 4.1 implies smaller the value of m, better the resilience. |s| is the size of the key pool.

The security analysis of the Basic scheme is calculated with memory as 3 and the key pool size as 900. As the number of nodes increases in the network, it is more probable that number of nodes being compromised also increases. Therefore, the resilience of the network increases with the decrease in the fraction of the nodes compromised.

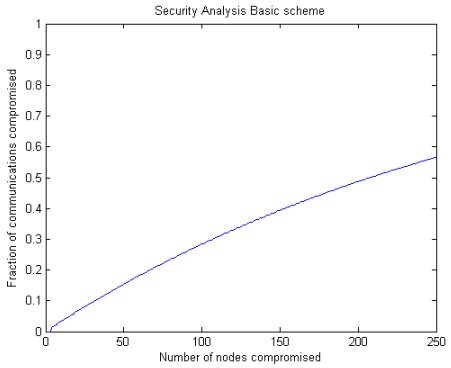


Figure 4: Security Analysis of Basic Scheme

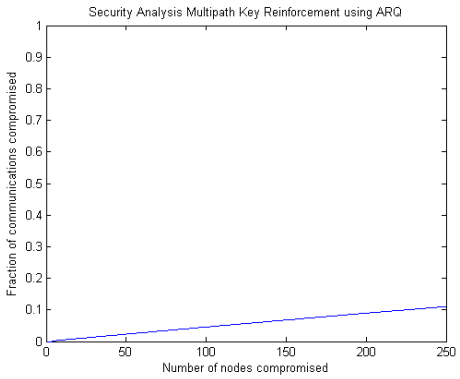


Figure 5: Security Analysis of Multipath Key Reinforcement

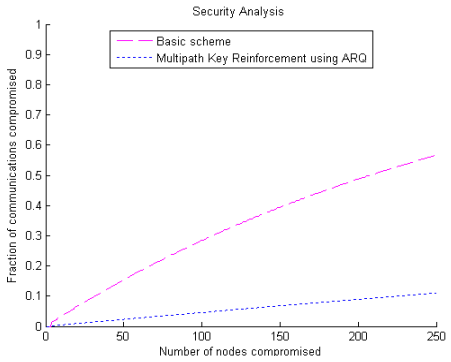


Figure 6: Security analysis comparisons

Figure 6 shows the comparison of security analysis of the basic scheme and multipath key reinforcement with memory as 3 and the key pool size as 1600. It is inferred that the resilience has increased as the number of nodes being compromised has decreased; eventually the security of the network also increases. The security of the Multipath Key Reinforcement is better than that of the Basic scheme.

From the results we infer that, the basic scheme is vulnerable to security threats leading to poor resilience. Whereas in the proposed scheme, the security is enhanced.

V. CONCLUSIONS

We have proposed and investigated a modified Incremental Redundancy Transmission (IRT) scheme for the secret common key establishment process of key pre-distribution techniques. The modified IRT scheme uses Selective Repeat ARQ mechanism to send the information through multiple multi-hop paths. An important feature of the IRT scheme is the flexibility of trading transmission for lower information disclosure. From the analysis, it can be inferred that multipath key reinforcement has proved to be a more tangible solution than the basic scheme in terms of resilience against node capture.

From the results and graphs it is inferred that the path availability is improved in the network, transmission overhead is reduced and security is enhanced in the proposed scheme.

In the future work we will consider transmission between multiple sources and multiple destinations and the effect of node disjoint paths will be investigated as well.

REFERENCES

[1] Eschenauer, L., Gligor, V.D. “A key-management scheme for distributed sensor networks,” In: Proc. Of the 9th ACM conference on Computer and communications security, Washington, DC, USA (2002)pp. 41–47

[2] Chan, H., Perrig, A., Song, D. “Random key predistribution schemes for sensor networks” In: Proc. Of IEEE Symposium on Security and Privacy, Berkeley, California (2003)pp.197–213

[3] Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J., Khalili, A. “A pairwise key pre-distribution scheme for wireless sensor networks,” ACM Trans. on Information and System Security 8 (2005) pp.228–258

[4] Jing Deng; Han, Y.S. “Multipath key Establishment for Wireless Sensor Networks Using Just-Enough Redundancy Transmission,” Dependable and Secure Computiong,IEEE Transactions(2008)pp.177-190