Adaptable Pre-Distribution Scheme for Keys in Wireless Sensor Networks

Rummana Firdaus
Department of Computer Science and Engineering,
GSSSIETW, India

***Abstract*- Key management is a challenging issue for Wireless Sensor Networks. One of the main concerns when designing a key management scheme is the network scalability.The protocol should support a large number of nodes to enable a large scale deployment of the network. A scalable key management scheme for WSNs should be adopted which provides a good secure connectivity coverage. For this purpose, the unital design theory is used. The basic mapping from unitals to key pre-distribution allows to achieve high network scalability but does not guarantee a high key sharing probability. Therefore, an enhanced unital-based key pre-distribution scheme is proposed.The proposed approach enhances the network scalability while providing high secure connectivity coverage and overall improved performance and reduces significantly the storage overhead compared to those of existing solutions.**

Keywords- Key management, Key Predistribution, Network scalability, Unital design, Wireless sensor network.

I. INTRODUCTION

Nowadays wireless sensor networks are increasingly used in numerous fields such as military, medical and industrial sectors. Due to resource limitations existing conventional solutions cannot be used in WSN. So security issues became one of the main challenges for resource constrained environment of WSN. Key management is a corner stone for many security services such as confidentiality and authentication which are required to secure communications in WSN. The establishment of secure links between the nodes is then a challenging problem in WSN. The public key based solutions which provide efficient key management services in conventional network, are unsuitable for WSN because of resource limitations. Symmetric key establishment is one of the most suitable paradigm for securing exchanges in WSN[1]. Because of lack of infrastructure there is no trusted third party which can attribute pair wise secret keys to neighbouring nodes, that is why most existing solutions are based on key pre-distribution[2]. The significant advances of hardware manufacturing technology and the development of efficient software algorithms make technically and economically feasible a network composed of numerous, small, low-cost sensors using wireless communications, that is, a wireless sensor network[4].

In the proposed system, scalability issue is tackled without degrading the other network performance metrics. For this purpose, a scheme has been designed which ensures a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency. To this end, the unital design theory for efficient WSN key pre-distribution is used.

A naive mapping from unital design to key pre-distribution is proposed and analytical analysis shows that it achieves high scalability. An enhanced unital based key pre-distribution scheme is proposed that maintains a good key sharing probability while enhancing the network scalability.

II. RELATED WORKS

Distributed Sensor Networks (DSNs) are ad-hoc mobile networks that include sensor nodes with limited computation and communication capabilities. DSNs are dynamic in the sense that they allow addition and deletion of sensor nodes after deployment to grow the network or replace failing and unreliable nodes. DSNs may be deployed in hostile areas where communication is monitored and nodes are subject to capture and surreptitious use by an adversary. Hence DSNs require cryptographic protection of communications, sensor capture detection, key revocation and sensor disabling.A key-management scheme is designed to satisfy both operational and security requirements of DSNs[5].

Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary. Mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node was presented[3]. First, in the q-composite keys scheme, the unlikeliness of a large-scale network attack in order to significantly strengthen random key predistribution's strength against smaller-scale attacks is trade off. Second, in the multipath-reinforcement scheme, the security between any two nodes is strengthened by leveraging the security of other links[3].

Wireless sensor networks are usually deployed to operate for a long period of time. Because nodes are battery-operated, they eventually run out of power and new nodes need to be periodically deployed to assure network connectivity. This type of networks is referred to as Multi-phase WSN in the literature [2]. A network that is temporarily attacked (i.e. the attacker is active only during a limited amount of time) automatically self-heals, i.e.

recovers its initial state when the attack stops. In contrast, with existing schemes, an attacker that corrupts a certain amount of nodes compromises a given fraction of the

total number of secure channels. This ratio remains constant until the end of the network, even if the attacker stops its action. Furthermore, with our scheme, a network that is constantly attacked (i.e. the attacker regularly corrupts nodes of the network, without stopping) is much less impacted than a network that uses existing key pre-distribution protocols. With these schemes, the number of compromised links constantly increases until all the links are compromised. With our proposal, the proportion of compromised links is limited and constant [6].

III. SYSTEM ARCHITECTURE

Fig 1 shows the system architecture. Service provider checks for the existence of all the nodes in the network. Router is responsible for data transfer between sender and receiver. It checks for attackers in the network by comparing the key present in its routing table with the attackers key. If the key matches then the node is not attacked , otherwise the node is attacked. The destination

verifies the key. If the key matches it accepts the data , otherwise it rejects the data.

3.1 Components of the system

3.1.1 Service Provider

Service Provider will check for the existence of nodes in the network. Once the nodes are found it initializes MAC address to them. It selects the file to be sent to the destination node. It is also responsible for generating and distributing keys. Two kinds of keys is generated by service provider.Deterministic Key which is a 128 bit key and is used whenever high security is required and Probabilistic Key which is a 16 bit key and is used whenever low security is required.

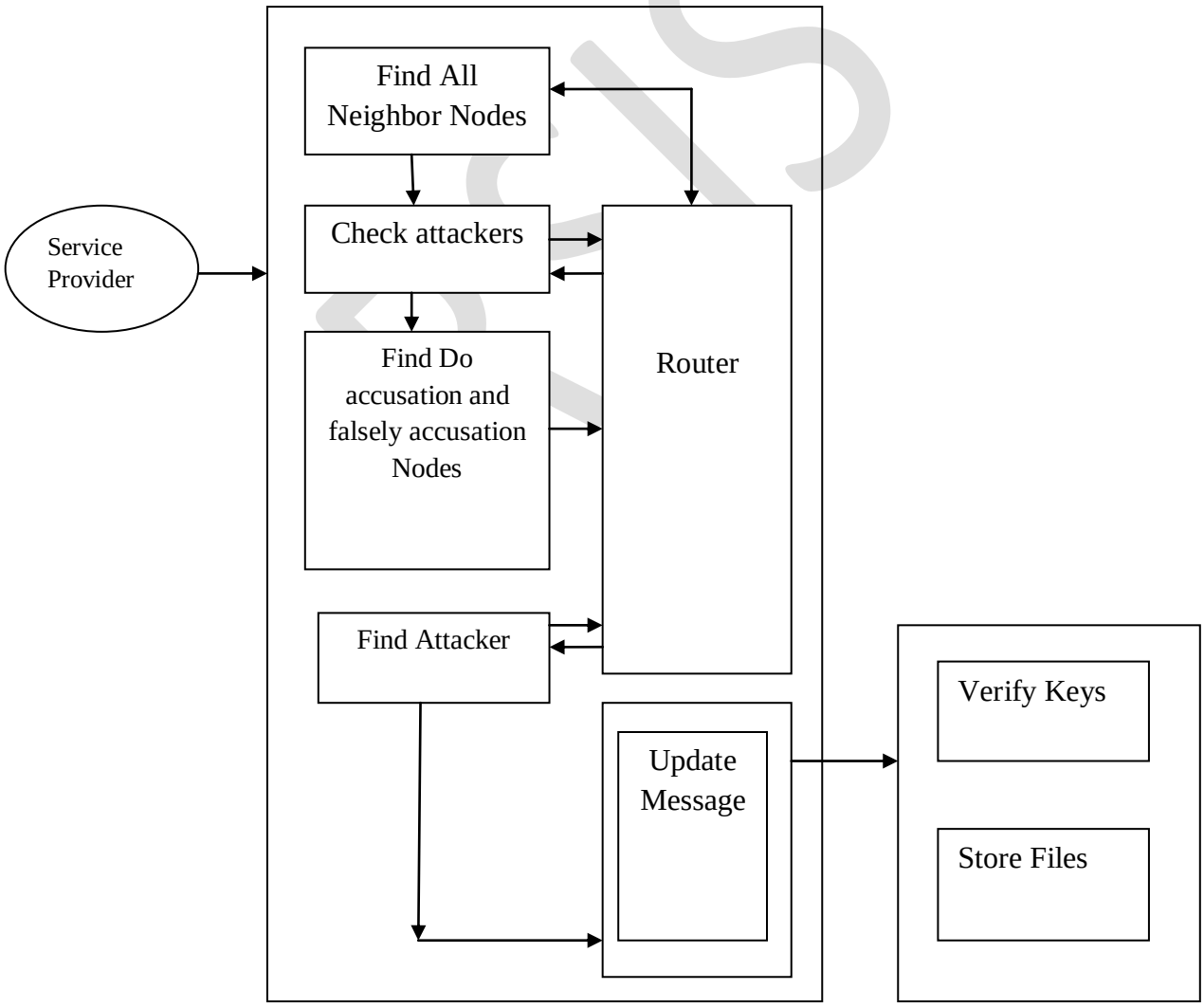

Fig. 1: System Architecture

3.1.2 Router

A router is a device that forwards data packets between computer networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. It is also responsible for distributing the keys to all the nodes in the network. Functions performed by router are assigning MAC address to the nodes in the network and finding the attackers by comparing the key present in its routing table with the attackers key.

3.1.3 Secure Transmission

Receiver receives the file sent by the sender. Upon receiving it verifies the key. If the key matches it accepts the data otherwise it rejects the data.

IV. CRYPTOGRAPHIC HASH FUNCTION

To achieve security in wireless sensor networks, it is important to he able to encrypt messages sent among sensor nodes. Keys for encryption purposes must he agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is nontrivial. Many key agreement schemes used in general networks, such as Diffie-Hellman and public-key based schemes, are not suitable for wireless sensor networks. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large[6]. SHA-1 a cryptographic hash function produces a 160 bit hash val.ue. A SHA-1 hash value is rendered as a hexadecimal number, 40 digits long. Even a small change in message will with overwhelming probability result in a completely different hash due to avalanche effect.

Step 1: Append Padding Bit

Message is "padded" with a 1 and as many 0's as necessary to bring the message length to 64 bits fewer than an even multiple of 512.

Step 2: Append Length

64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

Step 3: Prepare Processing Functions….

SHA1 requires 80 processing functions defined as:

f(t;B,C,D) = (B AND C) OR ((NOT B) AND D)

(0 <= t <= 19)

f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)

f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)

f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

Step 4: Prepare Processing Constants....

SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999 (0 <= t <= 19)

K(t) = 0x6ED9EBA1 (20 <= t <= 39)

K(t) = 0x8F1BBCDC (40 <= t <= 59)

K(t) = 0xCA62C1D6 (60 <= t <= 79)

Step 5: Initialize Buffers….

SHA1 requires 160 bits or 5 buffers of words (32 bits):

H0 = 0x67452301

H1 = 0xEFCDAB89

H2 = 0x98BADCFE

H3 = 0x10325476

H4 = 0xC3D2E1F0

Step 6: Processing Message in 512-bit blocks (L blocks in total message)

This is the main task of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks.

Input and predefined functions:

M[1, 2, ..., L]: Blocks of the padded and appended message
f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): 80 Processing Functions K(0), K(1), ..., K(79): 80 Processing Constant Words H0, H1, H2, H3, H4, H5: 5 Word buffers with initial values

Pseudo Code

For loop on k = 1 to L

(W(0),W(1),...,W(15)) = M[k] */* Divide M[k] into 16 words */*

For t = 16 to 79 do:

W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1

A = H0, B = H1, C = H2, D = H3, E = H4

For t = 0 to 79 do:

TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C,

C = B<<<30, B = A, A = TEMP

End of for loop

H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E

End of for loop

Output:

H0, H1, H2, H3, H4, H5: Word buffers with final message digest

V. CONCLUSION

A basic mapping from unitals to key pre-distribution allows to achieve an extremely high network scalability while giving a low direct secure connectivity coverage. An efficient scalable unital-based key pre-distribution scheme providing high network scalability and good secure connectivity coverage. The solution parameter is discussed and an adequate value giving a very good trade-off between network scalability and secure connectivity is proposed. RSA and AES algorithms can be encorporated to generate the keys.

The design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability (number of supported nodes), or degrade other performance metrics including secure connectivity, storage overhead and resiliency in the case of large networks.

In the proposed system, scalability issue is tackled without degrading the other network performance metrics. For this purpose, a scheme has been designed which ensures a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency. To this end, the unital design theory for efficient WSN key pre-distribution is used.

REFERENCES

[1] Walid Bechkit , Yacine Challal, Abdelmadjid Bouabdallah and Vahid Tarokh.A Highly Scalable Key Pre-distribution scheme for Wireless Sensor Networks.
[2] Castellucian C and A. Spognardi, A Robust Key Pre-distribution Protocol for Multi-Phase Wireless Sensor Networks.
[3] H Chan, A. Perrig, and D. Song, Random key pre distribution schemes for sensor networks.
[4] Y. Zhou, Y. Fang, and Y. Zhang, Securing wireless sensor networks.
[5] L. Eschenauer and V. D. Gligor, A key-management scheme for distributed sensor networks.
[6] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney A key management scheme for wireless sensor networks using deployment knowledge