Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-3, February 10, 2012

Route Diversity Based Optimal Path Selection Using Random Key Generation

Mageswari N
II ME CSE
Dept. of Computer Science & Engineering
Jayaram College of Engg & Tech,
Tiruchirappalli, India

Anitha P
Assistant Professor
Dept. of Computer Science & Engineering
Jayaram College of Engg & Tech,
Tiruchirappalli, India

Abstract - A network programming protocols provide an efficient way to update program images running on sensor nodes without having physical access to them. Securing these updates, however, remains a challenging and important issue, given the open environment where sensor nodes are often deployed. Several approaches addressing these issues have been reported, but their use of cryptographically strong protocols means that their computational costs (and hence, power consumption and communication costs) are relatively high. I propose a novel scheme to secure a multihop network programming protocol through the use of multiple one-way hash chains. The scheme is shown to be lower in computational, power consumption and communication costs yet still able to secure multihop propagation of program images.

Features:

- A cost-effective security scheme for network programming.
- Power consumption evaluation.
- A simple but effective method to counter tunnel (wormhole) attack.
- Immediate verification.
- Extensibility to other broadcast application in WSNs.

I. INTRODUCTION

Network programming is becoming necessary for WSNs because there is always a need to fix bugs in program images or insert new functionalities after WSN is deployed in an evolving, dynamic environment. Early network programming protocols concentrated on reliable program image dissemination and minimal end-to-end update latency using distribution methods having epidemic-like characteristics. However, they provided no authentication or security mechanisms. The absence of authentication of the broadcast of program image means that a malicious node could install arbitrary program images in the sensor nodes. An adversary could just capture one sensor node, inject malicious program images into the network, and thereby take control of the entire WSN.

The goal of this project is to present a design and implementation for a new scheme to verify the authenticity and integrity of program updates in network programming protocols. Our work is motivated by the following challenges. First, as a significant class of WSN sensor nodes is resource-impoverished, traditional cryptographic schemes are impractical. For example, the Tmote has 10 KB RAM, 48 KB flash memory, 1 MB storage, and 250 kbps communication bandwidth. This is barely sufficient to execute traditional asymmetric cryptography (e.g., RSA or Diffie and Hellman). It is important that a security scheme for WSNs should be low in power consumption and have low computational overhead. The second challenge arises from the open wireless environment in which WSNs are typically

deployed. Since program updates are also broadcast through the wireless medium, an adversary can readily intercept the program updates and attempt to forge a malicious program image while avoiding detection. Another complication arises from the way that sensor nodes are deployed.

Typically, these are left unattended after deployment, and as such are at risk of physical or functional capture. It is possible to physically secure a sensor network node against theft or tampering by a variety of means, but these physical approaches are outside the scope of this paper. This paper presents a scheme that is resilient against brute-force attack and node compromise.

1.1 OBJECTIVE OF THE PROJECT

I design, implement, and evaluate a novel scheme that meets the requirements of secrecy, authenticity, integrity, and freshness of broadcast messages in the context of a single-hop wireless sensor network. The contributions are three-fold: first, I propose the use of time-varying keys (based on a key-chain) for broadcast encryption, emphasizing advantages such as non-forge ability, protection against old-key compromise, and allowance for dynamic data. Second, I extend the basic key-chain mechanism to incorporate limited protection against key loss, allowing legitimate receivers to recover even if they have lost a small number of keys. Third, I prototype this scheme by incorporating it into Deluge, the network programming protocol distributed, and quantify its cost in terms of time.

1.2 BASIC CONCEPTS

1.2.1 User Profiles

- The user profile is represented as a set of categories, and for each category, a set of keywords with weights.
- The categories stored in the user profiles serve as a context to disambiguate user queries.
- The search can be narrowed down by providing suggested results according to the user preferred categories.

User profiling strategies can be broadly classified into two main approaches: document-based and concept based approaches.

1.2.1.1 Document-based methods

Focus on analyzing user's clicking and browsing behaviors recorded in the user's click through data. On web search engines, click through data are important implicit feedback mechanism from users. User's document preferences are first extracted from the click through data, and then, used to learn the user behavior model which is usually represented as a set of weighted features.

1.2.1.2 Concept-Based Methods

Concept based user profiling methods aim at capturing user's conceptual needs. These methods automatically derive user's topical interests by exploring the contents of the user's browsed documents and search histories that are automatically mapped into a set of topical

categories. User profiles are created based on the user's preferences on the extracted topical categories.

II. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

- A Network programming protocols concentrated on reliable program image dissemination and minimal end-to-end update latency using distribution methods having epidemic-like characteristics. However, they provided no authentication and security mechanisms.
- The absence of authentication of the broadcast of program image means that a malicious node could install arbitrary program images in the sensor nodes. An adversary could just capture one sensor node, inject malicious program images into the network, and thereby take control of the entire WSN.

2.2 PROPOSED SYSTEM

- This project is to present a design and implementation for a new scheme to verify the authenticity and integrity of program updates in network programming protocols.
- A significant class of WSN sensor nodes is resource-impoverished, traditional cryptographic schemes are impractical. It is important that a security scheme for WSNs should be low in power consumption and have low computational overhead.
- The open wireless environment in which WSNs are typically deployed. Since program updates are also broadcast through the wireless medium, an adversary can readily intercept the program updates and attempt to forge a malicious program image while avoiding detection.
- Another complication arises from the way that sensor nodes are deployed. Typically, these are left unattended after deployment, and as such are at risk of physical or functional capture.

III. SYSTEM DESIGN

3.1 MODULES

Module: 1 Packet preprocessing

In this module describes the packet preprocessing of the very first packet of program image. The omitted value of the first key chain is used to encrypt the next key element in the order of key dissemination (K1 in Figure 5.1). The encrypted result is the key update segment for the first hop group. Then, K1 is concatenated with P0 and the result is hashed, yielding the packet authentication segment. The key update segments and packet authentication segments for the successive hop groups are generated in the same way using their corresponding key chains. Finally, all these segments are concatenated with P0 as shown in Figure 5.3, giving the first packet to be transmitted. The way in which the key update and packet authentication segments are concatenated with the data packet is used in a countermeasure against tunnel attack. The above packet preprocessing procedure is repeated for successive packets in the image to be broadcast

Module: 2 Initialization and Key Predistribution

This scheme employs multiple one-way hash chains to secure the Deluge protocol (shown in the Figure 5.2). Hash chains1 are based on a function H with the property that its computation is easy, whereas its inverse H is extremely difficult to compute. A hash chain with length L is generated by applying H to an initial element repeatedly for L times. The last value after H has been applied L times is called the committed value of the hash chain. Before the sensor nodes are deployed, the base station constructs S hash chains. It generates S distinct random seed numbers and computes a one-way hash chain with length of L þ 1 starting from each seed, predistribution will not incur the overhead of a Diffie-Hellman key exchange protocol , and .key agreement between the base station and all sensor nodes would require Diffie-Hellman exchanges for each node if the Diffie-Hellman approach is adopted.

Module: 3 Security analysis

The nodes are assumed to be uniformly distributed. If an adversary wants to broadcast a malicious packet to k in our scheme successfully, it will have to compromise all the upstream neighbors of k. Otherwise, the compromised node will not have enough time to forge a malicious packet to circumvent our scheme . Similarly, estimates the number of nodes (i.e. downstream neighbors in the Figure 5.3) that might be affected by node k if node k is compromised. Assume that the sensor nodes are uniformly distributed the estimated number of upstream neighbors of node.

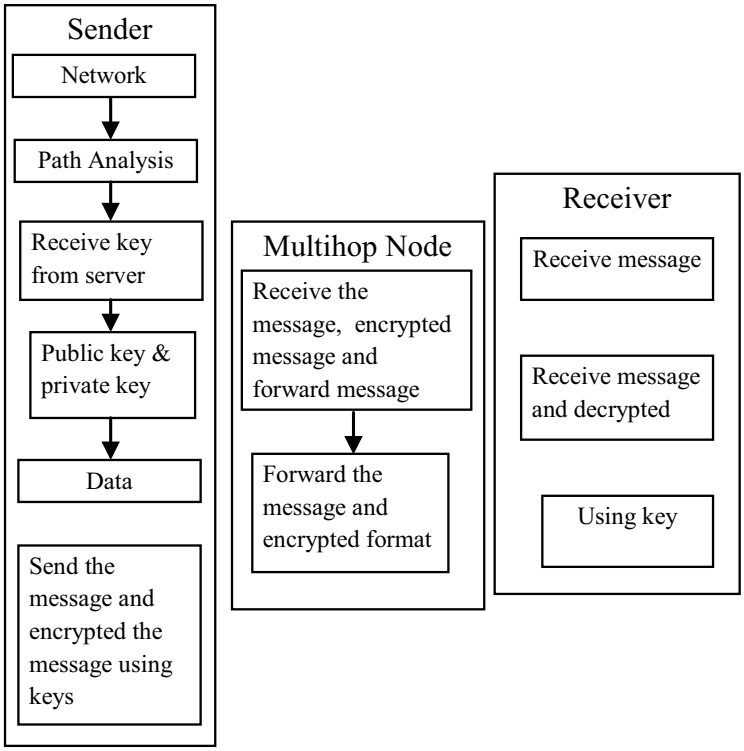
Attacker model

An adversary may compromise and fully control a subset of the sensor nodes, enabling him to mount various kinds of attacks. For instance, he can inject false data packets into the network and disrupt local control protocols such as localization, time synchronization, and route discovery process. Furthermore, he can launch denial-of-service attacks by jamming the signals from benign nodes. However, we place some limits on the ability of the adversary to compromise nodes. Note that if the adversary can compromise major fraction nodes of the network, he will not need nor benefit much from the deployment of replicas. To amplify his effectiveness, the adversary can also launch a replica node attack, which is the subject of our investigation. Assume that the adversary can produce many replica nodes and that they will be accepted as a legitimate part of the network. Also assume that the attacker attempts to employ as many replicas of one or more compromised sensor nodes in the network as will be effective for his attacks. The attacker can allow his replica nodes to randomly move or he could move his replica nodes in different patterns in an attempt to frustrate for proposed scheme.

Module: 4 Packet verification

In this section, the packet verification for the first data packet destined to the first hop group will be described (Figure5.4). The verification of subsequent packets in the other hop groups uses the same procedure with keys corresponding to those that were used in the packet preprocessing. After the preprocessing of a packet and the respective concatenation is transmitted to nodes in the first hop group. After retrieving the correct group information from P00, the sensor nodes verify the key update segment and packet authentication segments

3.2 Architecture Diagram



3.3 Module Diagrams

Module 1

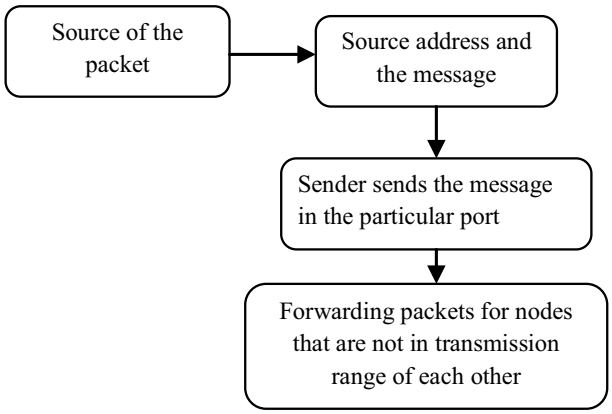


Figure 4.1: Packet Preprocessing

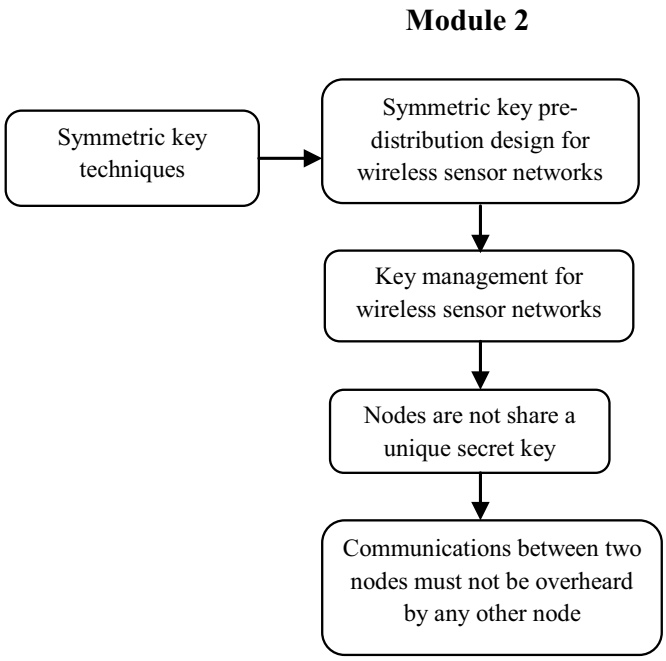


Figure 4.2: Initialization and Key Predistribution

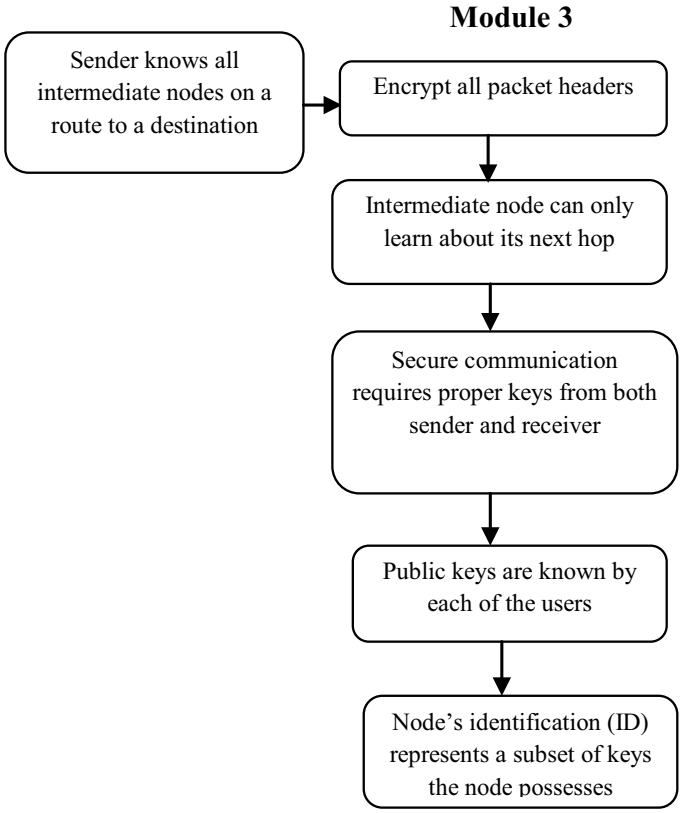


Figure 4.3: Security Analysis

Module 4

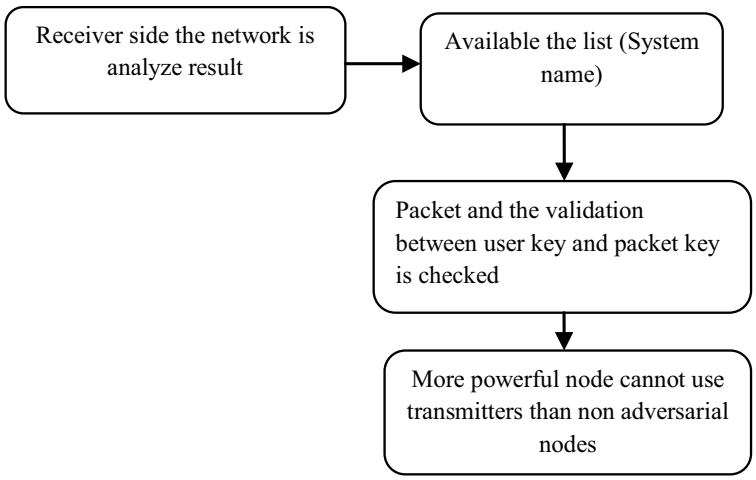


Figure 4.4: Packet Verification

IV. CONCLUSION

An authentication scheme, to secure multihop network programming by using multiple one way hash chains. Instead of the expensive asymmetric cryptographic primitives used in much prior work, in my proposed system employs only cryptographic primitives, in a circular geographic node deployment model. A comprehensive performance evaluation of scheme in terms of end- to- end latency and power consumption, which this is the first power consumption evaluation of a security scheme for network programming protocols.

REFERENCES

1. I. F. Akyildiz, E. Cayirci, Y. Sankarasubramaniam and W. Su, “A Survey on Sensor Networks,” IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.
2. D. Estrin, J. Heidemann and T. Stathopoulos, “A Remote Code Update Mechanism for Wireless Sensor Networks,” technical report, Univ. of California, Los Angeles, 2003.
3. D. Culler and J. Jeong “Incremental Network Programming for Wireless Sensors,” Proc. IEEE Conf. Sensor and Ad Hoc Comm. And Networks (SECON ’04), pp. 25-33, 2004.
4. R. Gandhi, P.E. Lanigan and P. Narasimhan, “Sluice: Secure Dissemination of Code Updates in Sensor Networks,” Proc. IEEE Int’l Conf. Distributed Computing Systems (ICDCS ’06), pp. 53-63, 2006.
5. L.M. Adelman, R.L. Rivest and A. Shamir, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Technical Report MIT/LCS/TM-82, 1977.
6. S. Jha , D.Ostry, J.Shaheen and V. Sivaraman, “Confidential and Secure Broadcast in Wireless Sensor Networks,” Proc. IEEE Int’l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC ’07), 2007.
7. Limin Wang and Sandeep S. Kulkarni “Authentication for Bulk Data Dissemination in Sensor Networks” Los Angeles, CA, November 2003.

8. Prentice Bisbal “Public Key Distribution and Authentication Using LDAP” IETF Networking Group, (April 2001)
9. Anuran Roy Chowdhury and Avik Modak “The Key Issues And Specifications For Designing An Appropriate Wsn “IEEE Comm. Mag., Aug. 2002, pp. 102–114.
10. Prof. S. Pallam Settyand O.Srinivasa Rao “Efficient Mapping Methods For Elliptic Curve Cryptosystems”Vol. 2(8), 2010, 3651-3656
11. Nilayam K Kamila, Prashanta K Patra, Prbodha K Pradhan and Prasant K Pattnaik “A Reverse Transmission Approach For Multi-Hop Routing In Wireless Sensor Network” vol 11 issue 6, 2004, pp 6-28.
12. Mohd. Uruj Jalil “ Robust Energy Management Routing in WSN using Neural Networks” Volume: 02, Issue: 04, Pages: 788-791(2009)
13. Ashok M. Kanthe “Power Control through Non cooperative Game Theory on Wireless Sensor Network” vol. 2, pp. 808-817, Apr. 2003.
14. Gerald Wagenknecht , Markus Anwander and Torsten Braun “Energy-efficient Management of HeterogeneousWireless Sensor Networks” Appl, (2003) 6067
15. Anna Lysyanskaya and Jan Camenisch “A Signature Scheme with Efficient Protocols” Springer Verlag, 2000.
16. Khalid N Chaaran , Munzza Younus and Muhammad Younus Javed “NSN based Multi-Sink Minimum Delay Energy Efficient Routing in Wireless Sensor Networks” Vol.41 No.3 (2010), pp.399-411
17. Guangbin Wu ,Weihua Guo and Zhaoyu Liu “An Energy-Balanced Transmission Scheme for Sensor Networks” Florida, March 2002.
18. Chandrashekhar Meshram “Modified ID-Based Public key Cryptosystem using Double Discrete Logarithm Problem” Vol. 1, No.6, December 2010
19. E. Bresson1, O. Chevassut2,3, O. Pereira2,D. Pointcheval1 and J.-J. Quisquater2 “Two Formal Views of Authenticated Group Diffie-Hellman Key Exchange” February 28, 2002
20. Anish Arora and Sandip Bapat “Stabilizing Reconfiguration in Wireless Sensor Networks” vol. 26,pp. 565–569,2004.