Graduate Research in Engineering and Technology (GRET)

Volume 1 | Issue 2 Article 10

October 2013

SECURING MULTIHOP NETWORK BY DETECTING AND LOCATING POLLUTION ATTACKS USING SPACEMAC.

ANUPAMA. T. .A
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India., anupamata@gmail.com

R APARNA Dr.
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India., r_aparna@gmail.com

SECURING MULTIHOP NETWORK BY DETECTING AND LOCATING POLLUTION ATTACKS USING SPACEMAC.

ANUPAMA.T.A[1], DR. R APARNA[2]

[1]M.Tech Student, [2]Associate Professor
Department of Computer Science and Engineering, Siddaganga Institute of Technology,
Tumkur, Karnataka, India.

Abstract- It has been widely observed that providing security is one of the challenging task in Wireless sensor network(WSN). Program images need to be updated continuously as network programming happens in WSN. Many Networking protocols provide an efficient way to update these program images running on sensor nodes. One of the cryptographically strong protocol called DELUGE exists to address this challenge, but it involves high computational cost such as power consumption and communication costs. So Multiple one way key chain is proposed to secure a multihop network programming protocol which is lower in power consumption and communication costs. Even though one way key chain is used to provide security, network with static topology is considered. Network is made dynamic by adding mobility nodes to it. But the extra node added may not always be the genuine node. If it is an attacker node, there can be several pollution attacks. Attacker node travels through the network, and pollute the entire network. Wirelesss sensor network may not be able to detect these pollution attacks. In this paper, we are proposing a MAC scheme called Spacemac. It expands the network by adding nodes to it. Using SpaceMac, i) it detects the polluted packets early at the intermediate nodes. ii) it identifies the exact location of an attacker and eliminates them.

Keywords- *Network programming protocols, cryptographic protocols, sensor network security, pollution attacks, attack detection, homomorphic MAC, network coding, message authentication.*

I. INTRODUCTION

Network programming has become necessary for wireless sensor network (WSN) because image update may be subsequently required for bug fixes or to provide new functionalities after a WSN has been deployed in an evolving, dynamic environment.

Initial network programming protocols [2], [3], [4], [5] concentrated on reliable program image distribution and minimal end-to-end update latency. But they did not provide authentication and security mechanisms. The absence of authentication in broadcast of a program image imposes a vulnerability to installation of arbitrary program images in WSNs. An adversary can simply capture one sensor node in

WSNs and inject a malicious program image. Without a proper authentication mechanism, an adversary can take control of the entire WSN with minimal effort.

In an open wireless environment, WSNs are typically deployed. Since program updates are broadcasted 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. Due to the inherent weakness of network coding, malicious node could inject corrupted packets into a network which gets combined and forwarded by downstream nodes, thus causing a large number of corrupted packets propagating in the network. This prevents the decoding of original packets at the receivers.

In order to overcome the above security issues, in this paper we propose a method for detecting and locating the pollution attacks. Inherent weakness of network coding causes pollution attacks. A homomorphic MAC scheme called SpaceMac is introduced, which detects and locates the polluted packets at the early intermediate node itself. Here SpaceMac is also used for expanding the network. The Network coding paradigm defines that intermediate nodes in a network should mix incoming packets with other packets instead of simply forwarding them, and receivers should decode to obtain the original packets. This idea, originally introduced by Ahlswede et al. [1]. Here we consider the packets arriving from the same source node i.e, intra-session linear network coding.

The rest of the paper is organized as follows. Section II provides an overview on related work. Then we present our proposed method with system model in Section III. In Section IV, we give the implementation details of proposed system. In section V, we analyze the security of proposed method. Lastly we conclude the paper in Section VI.

II. RELATED WORK

In this section, we review one of the most popular multihop network programming protocol called Deluge[2]. Deluge divides the program updates into fixed size pages, which are further divided into fixed sized packets. Here packets are the basic transmission units. Nodes distribute the pages in a pipelined fashion. Nodes forward the pages that they have completely received. It cannot forward a page without having received all previous pages.

Since the program image is composed of pages, where each page consists of series of packets. Secure network programming protocols computes hash function of the last packet [10] and attaches its hash to the previous packet. The packet with the hash is hashed and attaches it to its previous packet. This process continues until the first packet is reached. Now the private key of the base station is attached to the first packet and send to the receiver node. Each receiving sensor node verifies the first packet with the base station's public key, then recursively authenticates each packet or page using the hashed value from the previous packet/page until the entire program update has been successfully received. Digital signature is used here which incurs high computational overhead.

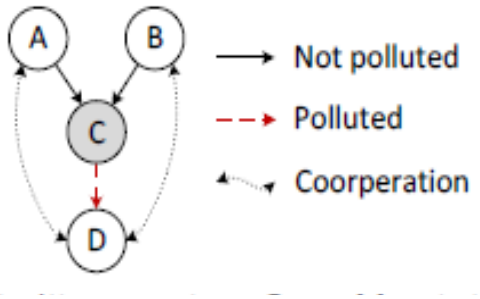
Jaleel et al. proposed one way key chain to provide confidentiality of program updates [13]. Inorder to reduce the high power consumption, Lanigan et al. have proposed symmetric cryptography [14], [15]. It is used to authenticate broadcast program updates. It works in the following manner. Base station divides the network by grouping the nodes. All the node are registered at the base station. Base station assigns symmetric key to each group. Same symmetric key is used by all the nodes in a group. To move from one group to another, node from the first group asks for the symmetric key of next group. It then compares the key with the node in the second group, if it matches, it moves from one group to another group. By doing like this, packets can be verified. Packets are immediately verified as and when they are received. Number of packets to be broadcasted is not to be known earlier. Just base station has to generate long enough key chains to cover the lifetime of wireless sensor network.

Till now we have considered the nodes that are static in nature, i.e WSN of static topology is considered. In our scheme we are expanding the network by adding extra nodes to it. The nodes that are added may inject corrupted packets into the network. These corrupted packets combines with other packets in the network and pollutes the entire WSN. Mac scheme called SpaceMac is introduced. It first verifies whether the received packets belongs to a specific network even if the network gets expanded. The scheme identifies the attack at the intermediate node itself. It does not allow polluted packets to swan through the entire network. SpaceMac allows intermediate nodes to send only linear combinations of packets that they receive from their parents. Here parent and child node of any intermediate node cooperate to detect the corrupted packets. Kehdi and Li [16] propose in network detection scheme. In this scheme integrity is verified by checking whether the packets belongs to the network spanned. Rodriguez [8] probabilistic checking and cooperative mechanisms among nodes t reduce computational overhead. Two homomorphic MAC schemes are proposed by 2 groups of researcher: Agarwal &Boneh [6] and Li et al [7]. Both the schemes have low computational overhead since they require only simple addition and multiplication operations at intermediate nodes for both MAC identity and identity verification.

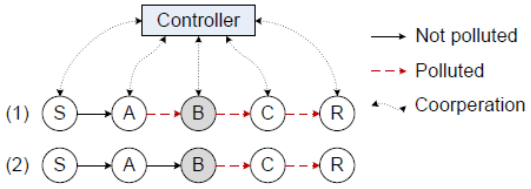
III. PROPOSED SYSTEM

In this section, we present a MAC scheme called SpaceMac which makes a static network as a dynamic network and provides security to it from pollution attacks. .

A. System Model



Above diagram shows how SpaceMac helps to detect pollution attacks. Using SpaceMac, A and B are able to sign the expanding space. D is able to verify any packet sent by C to see if it belongs to expanded space . If there is a packet sent by C that is not in expanded space the attack is detected by D. The cooperation among A, B, and D helps detect the attack from C.



Above diagram shows the attacker's location. The attacker is at the node B. controller narrow down the attacker to the two candidate nodes A and B. Cooperation among the nodes and the controller helps the locating process.

Let us consider the threat model:

Threat Model:
Here we assume both the source and receivers are trustworthy but the intermediate nodes may be malicious. We assume that network may have many pollution attackers. They can be located at the intermediate nodes in the network. Each attacker injects corrupted packets to the network and corrupts the entire network. They may also modify other data such as authentication tags. If the data is modified successfully, attack is said to be tag pollution.

IV. IMPLEMENTATION

Here we construct a MAC scheme called SpaceMac. The construction of this scheme is new and is more efficient in detecting and locating pollution attacks. SpaceMac verifies the network as and when it expands over time. It is designed for the low computational overhead i.e, system should use less amount of time for computing.

Detection operation is implemented by using 3 algorithms : Mac, Combine and Verify.

- Mac : Mac algorithm generates an identity or tag for a given network.
- Combine : Combine algorithm computes identity for linear combination of network.
- Verify: Verify algorithm verifies whether the identity is a valid identity of a given network.

Our Detection scheme works as follows:

Base station knows the complete topology of the network. The base station could be the source node itself. This assumption is made in the recent work by Li et al [11]. Each nodes share a pair of secret keys with base station. In SpaceMac, base station determines the key KN, which is secret to node N and is used by packets and children node of

N. A node can either be a parent node or a child node. But it is required to know a different set of keys participating in the detection. Source and all receivers need to share end to end key, K. This is used in case of adversaries attack. Base station sends packet consisting of the set of keys to each node that participate in the detection scheme. It is sent through a secure and authenticated channel. The source S calculates an end to end tag using Mac algorithm of SpaceMac before sending out the source packets. Source attaches this tag to every source packet. These are the linear combinations. Let us consider an example, Assume that the parent P wants to send a packet y to its child N. Child node N has to detect the corrupted packets, so parent node P calculates helper tag and give it to the child node. Before sending a packet, parent P needs to calculate MAC tag using Mac. Parent sends helper tag along with the verification tag of y, which is used by N to verify the integrity of y.

The verification tag will be computed correctly because the Combine algorithm linearly combines the tags in the same way the packets are combined. At the receiver node, Verify algorithm is used to verify the integrity of the packet. If non linear combination packets are arrived, attacks are immediately detected.

Location scheme works as follows:

SpaceMac is used to prevent nodes from lying about their received spaces. MAC algorithm defines a secret key which is shared between a node and the controller. Linear combination packets are generated. Controller collects the true subspaces from every node. This prevents nodes from lying. By boing so exact location of an attacker node can be known.

V. SECURITY ANALYSIS

In this section, we are providing some of the security features that are met in our scheme.

- Scalability: Our scheme achieves scalability. Here we can make static network as a dynamic network using SpaceMac.
- Data Integrity: Space Mac uses Mac, Combine and Verify. It checks for the corrupted packets. By using these 3 set of algorithms data integrity is achieved..
- Communication overhead: SpaceMac doesnot depends on the packet size. Digital signature is not
- used, symmetric keys are distributed. Mac keys are used for multiple source generations using SpaceMac. As a result, overhead is negligible.

Experimental Results:

Here we are comparing SpaceMac scheme with Deluge [2].

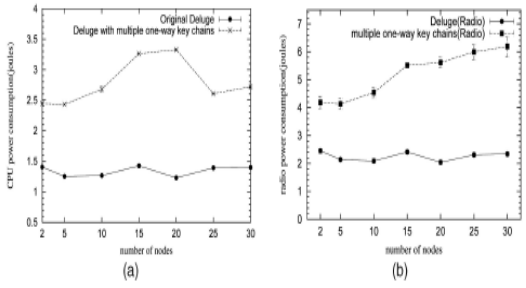


Fig: Power consumption for Deluge [2] and our scheme.

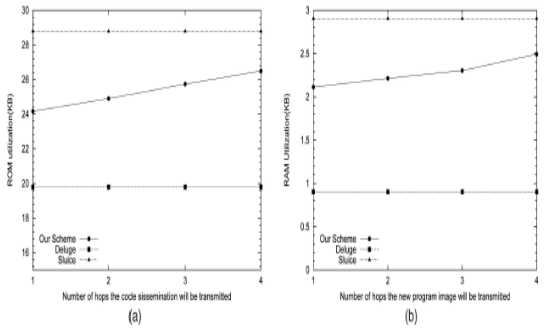


Fig: Memory Overhead in Deluge [2] and our scheme. (a) ROM usage and (b) RAM usage

VI. CONCULISON

In this paper, we introduce a novel homomorphic MAC scheme for expanding space called SpaceMac. We propose a cooperative defense system against pollution attacks built on SpaceMac. It detects and locates the pollution attacks in time. Computational costs such as communication costs, memory overhead and power consumption are reduced.

REFERNCES

[1] R. Ahlswede, N. Cai, S.-y. R. Li, and R. W. Yeung, "Network information flow," IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] J.W. Hui and D. Culler, "The Dynamic Behavior of a Programming at Scale," Proc.Int'l Source Conf. Embedded Networked Sensor Systems (SenSys '04),pp. 81-94, 2004.

[3] T. Stathopoulos, J. Heidemann, and D. Estrin, "A Remote Code Update Mechanism for Wireless Sensor Networks," technical report, Univ. of California, Los Angeles, 2003.

[4] L. Wang, "MNP: Multihop Network Reprogramming Service for Sensor Networks," Proc. Int'l Source Conf. Embedded NetworkedSensor Systems (SenSys '04), pp. 285-286, 2004.

[5] J. Jeong and D. Culler, "Incremental Network Programming for Wireless Sensors," Proc. IEEE Conf. Sensor and Ad Hoc Comm. And Networks (SECON '04), pp. 25-33, 2004.

[6] S. Agrawal and D. Boneh, "Homomorphic MACs : MAC-Based Integrity for Network Coding," in ACNS'09, 2009.

[7] Y. Li, H. Yao, M. Chen, S. Jaggi, and A. Rosen, "RIPPLE.Authentication for Network Coding," in IEEE INFOCOM'10, 2010

[8] C. Gkantsidis and P. R. Rodriguez, "Cooperative Security for Network Coding File Distribution," in IEEE INFOCOM'06, 2006.

[10] P.K. Dutta, J.W. Hui, D.C. Chu, and D.E. Culler, "Securingthe Deluge Network Programming System," Proc. Int'l Conf. Information Processing in Sensor Networks (IPSN '06), pp. 326-333, 2006

[13] J. Shaheen, D. Ostry, V. Sivaraman, and S. Jha, "Confidential and Secure Broadcast in Wireless Sensor Networks," Proc. IEEE Int'l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC '07), 2007.

[14] D.H. Kim, R. Gandhi, and P. Narasimhan, "Exploring Symmetric Cryptography for Secure Network Reprogramming," Proc. Int'l Conf. Distributed Computing Systems Workshops (ICDCSW '07), p. 17, 2007

[15] P.E. Lanigan, P. Narasimhan, and R. Gandhi, "Tradeoffs in Configuring Secure Data Dissemination in Sensor Networks: An Empirical Outlook," Technical Report 006, Carnegie Mellon Univ., May 2007.

[16] E. Kehdi and B. Li, "Null Keys : Limiting Malicious Attacks Via Null Space Properties of Network Coding," in IEEE INFOCOM'09, 2009, pp. 1224–1232.

[17] A.Le and A. Markopoulou, "Cooperative Defense Against pollution Attacks in Network Coding Using SpaceMac," in Technical Report [Online]. Available: http://arxiv.

[20] Jafarisiavoshani, C. Fragouli, and S Diggavi, "Subspace properties of Randomized Network Coding".

◈◈◈