A Survey on Hybrid Wireless Mesh Protocol Security

Whye-Kit Tan, Sang-Gon Lee *, Jun-Huy Lam
Department of Ubiquitous IT, Division of Computer and Information Engineering,
Dongseo University, Busan, Korea
* Corresponding Author
whyekit.tan@gmail.com, nok60@dongseo.ac.kr, timljh@gmail.com

Abstract

Wireless Mesh Network (WMN) functionality had been included into IEEE 802.11s. For WMN, the routing message is one of the most important parts that need to be protected. Hybrid Wireless Mesh Protocol (HWMP) is the default routing protocol for WMN. In this paper, the attacks and vulnerabilities of HWMP had been identified and the requirements needed to protect HWMP had also been discussed. Existing HWMP security had been compared with the requirements.

1. Introduction

Wireless Mesh Network (WMN) as described in the IEEE 802.11s protocol is still in the development process. One of the interesting topics for this protocol is regarding the routing security. The routing is managed by formation of paths for data transmission within the mesh network.

WMN provides a lot of advantages to network but securing the network is more challenging especially for routing protocol [1]. The security for HWMP is not defined in the IEEE 802.11s draft [2], [3]. The draft had only detailed out the Robust Security Network Authentication (RSNA) method such as Simultaneous Authentication of Equal (SAE) [4] and how keys can be derived. More researches are needed to find a way to secure the HWMP. This paper explores the vulnerabilities of HWMP and attacks that can be performed on it. Security requirements to prevent the attacks will also be discussed.

2. Vulnerability of HWMP

There are many types of attack that can be done to a network. This section will discuss about the types of attack that can be done on HWMP.

2.1. Types of Attacks

Attackers can perform eavesdropping on HWMP frames to collect routing information. If the routing paths are known, it will be easier for attackers to plan their further attack.

It is possible to flood a WMN with path request (PREQ) frames by selecting a target mesh station (STA) address that does not exist in the network [5]. With this, the PREQ frame will sure be propagated continuously until the Time to Live (TTL) timed out. If the attackers continuously send out this kind of PREQ, the network will be flooded with PREQ frames eventually.

Data modification can done by intercepting messages and modify the messages before sending them back to the receiver. This kind of attack can cause major problem to a network without the users realizing about it. HWMP frames can be modified to disturb the WMN routing.

Identity spoofing is done by impersonating the identity of a user. The identity can be IP address or MAC address of a user. In poor security network, an attacker can easily impersonate another user by using its identity. In 802.11s based WMN, authentication is needed before a mesh STA can join the network; if RSNA is enabled. However, the draft does not explain about how to authenticate HWMP frames.

2.2. Attacks From Outside and Inside

In normal case, network security is supposed to protect a network from outside attack. Outside attack means that the attacker does not belong to the network and has no access to the network. The intention for outside attack is usually to disrupt the service of the network. This is especially true if the attack is done on the network's routing.

Inside attack is the opposite of outside attack. It is performed by authorized users of the network. The attacker has the password and is able to use the service provided by the network. Bandwidth of a WMN is limited and it must be shared by all mesh STAs. One way to rob the bandwidth from the network is to deny the service of other clients. The selfish attacker can perform denial of service onto other clients by dropping their packets intentionally [5]. However, this requires the attacker mesh STA to become the intermediate mesh STA for the clients. Therefore, attacker must attack the HWMP frames to ensure that all routing paths will go through him.

3. Mutable and Non Mutable Fields

Figure 1 shows the format of PREQ, RANN, and PREP frames which involve directly in the path discovery process. The darken fields are mutable field (MF) that need to be changed every time the frames are propagated while the rest are non mutable fields (NMF) that shall not be changed when the frames are propagated [6]. PREQ and RANN are broadcast frames while PREP is unicast frame. The ways to protect MF and NMF are different.

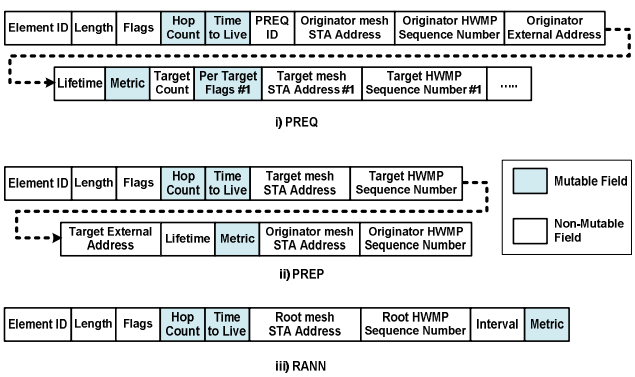

Figure 1. PREQ,PREP and RANN

4. Security Requirements to Prevent Outside Attacks

Link to link security relies on the trust between mesh STAs. Each transmission is secured in term of links. In multi hopping path, the transmission through the path is assumed to be secured if and only if all the mesh STAs involved in the transmission is trustworthy. Link to link security is sufficient to protect HWMP against outside attack.

Encryption is the way to protect against eavesdroppers. PREP frame is a unicast frame used to confirm a path while PREQ and RANN are broadcast frames used to find a path. By capturing the metric, transmitter and receiver address, an eavesdropper can figure out the routing paths. Therefore, the MF of HWMP frames must be encrypted. Since PREP is a unicast frames, its NMF will also reveal routing path thus it must also be encrypted.

As for data modification, impersonation, and flooding attack, it is sufficient to protect against these attacks by providing authentication and integrity to the HWMP frames in a link to link manner. It must be assumed that all the mesh STAs in the WMN are trustworthy. This will ensure that only authorized mesh STAs in the WMN can transmit HWMP frames.

The security features needed to protect HWMP from outside attack had been summarized and tabulated into Table 2. Usually, encryption is not needed for broadcast frames but it is needed for the mutable fields to protect the routing information from being revealed.

Table 1. Security features needed to protect against outside attacks (Link to link based security)

Frame	Fields	Authentication	Integrity	Encryption
PREQ *(Broadcast)*	MF	Need	Need	Need
	NMF	Need	Need	Not Needed
RANN *(Broadcast)*	MF	Need	Need	Need
	NMF	Need	Need	Not Needed
PREP *(Unicast)*	MF	Need	Need	Need
	NMF	Need	Need	Need

5. Existing HWMP security

Md. Shariful Islam et al. [6] had proposed Secure Hybrid Wireless Mesh Protocol (SHWMP) to protect the HWMP frames. Their proposed security protocol is a link to link security approach that is able to protect HWMP against outside attack but not inside attacks.

Pairwise Temporal Key (PTK) and Group Temporal Key (GTK) are both authenticated keys produced by RSNA protocol. Therefore, the key is unique and can be used to ensure the authentication of frames transmission. PTK is used for unicast frames while GTK is used for multicast/broadcast frames. Authentication provided by these keys is a link to link authentication. It will still suffer from the untrustworthy intermediate mesh STA problem.

SHWMP utilized merkle tree to generate Message Integrity Code (MIC) over the MF. This will protect the integrity of the MF. After that, PTK/GTK will be used to create a Message Authentication Code (MAC) over the MIC. This ensures the authentication and integrity of the MF. Lastly, PTK/GTK will also be used to encrypt the NMF to provide confidentiality.

Table 2. Security features provided by SHWMP

Frame	Fields	Authentication	Integrity	Encryption
PREQ *(Broadcast)*	MF	Yes	Yes	No
	NMF	Yes	No	Yes
RANN *(Broadcast)*	MF	Yes	Yes	No
	NMF	Yes	No	Yes
PREP *(Unicast)*	MF	Yes	Yes	No
	NMF	Yes	No	Yes

Table 2 shows the securities features provided by SHWMP. The highlighted parts are parts where features are needed but not provided by SHWMP.

6. Conclusion

WMN relies on its routing protocol to work in multi hopping environment. HWMP enable two mesh STAs that are far apart to communicate with each other. Therefore, it is very important to keep the HWMP secured but securing multi hopping path is very challenging.

Attacks can come from outside or inside of the network. Link to link security is sufficient to protect HWMP from outside attack. However, it is not easy to provide security against inside attack.

Currently, the WMN authentication is done in a link to link manner. Therefore, the security scheme must also works in the same way. This limits the way to provide protection to the routing messages.

Acknowledgement

This work was supported by 2011 National Research Foundation of Korea (2011-0004713).

References

[1] Ping Yi, Yue Wu, Futai Zou and Ning Liu. ”A Survey on Security in Wireless Mesh Networks”. IETE, February 18, 2010.

[2] IEEE P802.11s/D4.01, “Draft STANDARD for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements – Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, February 2010.

[3] Wang, X., Lim, A.O.: IEEE 802.11s Wireless Mesh Networks: Framework and Challenges. In: AdHoc Networks, pp. 1–15 (2007), doi:10.1016/j.adhoc. 2007

[4] D. Harkins. “Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks”, SENSORCOMM Conference Sensor Technologies and Apps. August 2008.

[5] Hui Lin, Jianfeng Ma, Jia Hu, and Kai Yang, “PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks”, EURASIP Journal on Wireless Communications and Networking 2012, doi:10.1186/1687-1499-2012-69, 28 February 2012.

[6] Md. Shariful Islam, Md. Abdul Hamid, and Choong Seon Hong, “SHWMP: A Secure Hybrid Wireless Mesh Protocol for IEEE 802.11s Wireless Mesh Network”, Transaction on Computational Science VI, LNCS 5730, pp. 95–114, 2009.