International Journal of Information & Network Security (IJINS)
Vol.2, No.2, April 2013, pp. 167~176
ISSN: 2089-3299

Hierarchical Wireless Mesh Networks Scalable Secure Framework

K. Ganesh Reddy, P. Santi Thilagam
Departement of Computer Science and Engineering, National Institute of Technology Surathkal

Article Info

Article history:

Received Sep 25th, 2012
Revised Nov 20th, 2012
Accepted Dec 10th, 2012

Keyword:

First keyword
Second keyword
Third keyword
Fourth keyword
Fifth keyword

ABSTRACT

Wireless Mesh Networks (WMNs) are more scalable than any other wireless networks, because of its unique features such as interoperability, integration and heterogeneous device support. Lacks of robust existing services in WMNs all the features are more vulnerable to various types of attacks. Hence, protect the scalability of WMNs against adversary nodes is a major issue. In this paper, we design Scalable Secure Framework (SSF) to address the scalability issue in WMNs. SSF is designed two algorithms: router authentication and deauthentication on backbone mesh to protect against unauthorized access and colluding attackers. SSF also secures integration and interoperability features of WMN by enhancing security features in 802.11s and Wi-Fi. Eventually security analysis results show that SSF effectively protects against imprinting, replay attack and node deprivation attacks.

Corresponding Author:

K. Ganesh Reddy,
Departement of Computer Science and Engineering,
National Institute of Technology Surathkal, India.
Email: guncity11@gmail.com

1. INTRODUCTION

Wireless mesh networks (WMNs) have emerged as a key technology for providing fast and hassle free services to users and inspiring numerous applications. In recent years, wireless mesh networks have been becoming more popular because of its ubiquitous broadband wireless internet connectivity in a sizable geographic area and cost effective network deployment. WMNs have unique features such as integration, interoperability and Ad-Hoc features Figure.1. depicts the three level hierarchy of wireless mesh network architecture [1],[2],[7],[12]. Here all wireless radio nodes are connected multi-hop faction to form infrastructure mesh as well as client mesh in which nodes are ordered hierarchy: gateway, router, and mesh client.

WMNs are more scalable because mesh routers provides interoperability and integration features among different wireless networks such as high-speed metropolitan area mobile networks, backhaul connectivity for cellular radio access networks, intelligent transport system network defense system and citywide surveillance systems. Other hand WMNs are more vulnerable to various types of attacks due to lack of robust security frameworks [9],[11],[13],[15] [16]. In this paper, we have done the comparison study of existing mechanisms with five different scalable features. In WMNs, first, two features with respect to protect against unauthorized and colluding attacks in WMN. The last three features are representing three level hierarchy, heterogeneous network/devices and decentralized authentication features in WMNs. We found that none of the existing mechanism is adequate to support all the features. We have designed Scalable Secure Framework (SSF) to provide all the five scalable features in WMNs. SSF mainly considers three level authentication by supporting all the five scalable features.

In three level hierarchy, Gateways are connected through conventional wired network which are placed on level one. Compare to the wireless networks, wired networks are more secure due to their standard available security protocols[17],[18]. We considered one of the strand wired security protocol (IPsec) to establish mutual authentication between gateways. Gateways start exchange the routers information securely after successful gateways authentication.

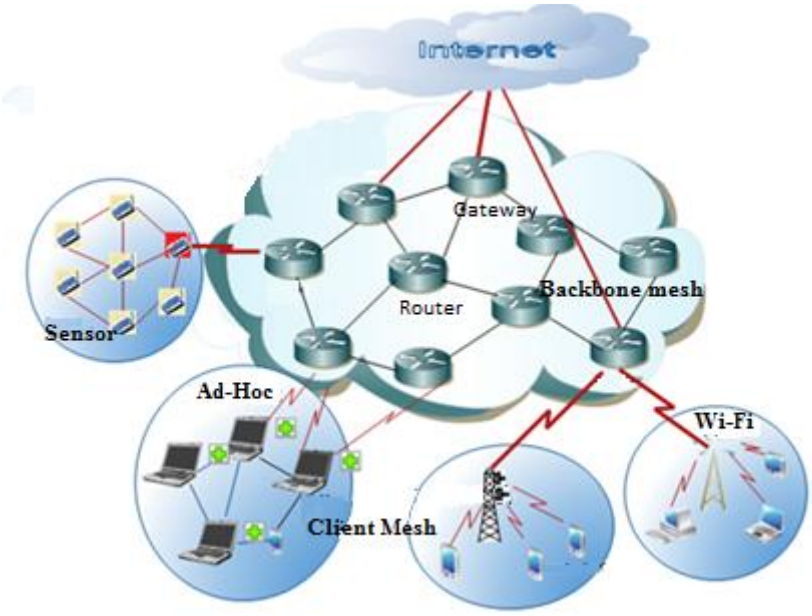

Figure 1. Wireless mesh networks architecture

We have designed two algorithms at router (second) level for authentication and deauthentication of a router. These two algorithms protect against multiple attacks and unauthorized nodes. Third level, SSF considers two different client mesh networks such as 802.11s [8] and Wi-Fi [13] to support integration and interoperability. We identify the drawbacks of 802.11s and Wi-Fi security mechanisms. SSF have enhanced security of 802.11s and Wi-Fi by overcoming existing drawbacks in our proposed SSF.

The rest of this paper is organized as follows. Section 2 introduces some preliminaries. Comparative study of existing mechanisms is discussed in section 3. Discuss the Design of Scalable Secure Framework in Section 4. Security analysis of SSF is explained in Section 5. Section 6 concludes the paper.

2. PRELIMINARIES

SSF has been developed based on five different scalable networks features. First two features are about protecting against of unauthorized nodes and colluding attacks. Distributed authentication, heterogeneous network/device support and three-level hierarchy are the other three scalable features in SSF. We discussed all the five features briefly in the following:

Protect against unauthorized nodes: Unauthorized (external) nodes do not have network access. However, these nodes are misusing network resource by illegal network access. WMNs need proper authentication mechanisms to protect against unauthorized node from whole network.

Protect against colluding attack: Two or more adversaries work together to isolate the legitimate node from WMN. Here, colluding adversaries isolate legitimate node by blocking the data or authentication packets to the particular destination nodes. Colluding attack severely affect the scalability of WMNs and difficult to prevent or detect colluding attack.

Heterogeneous network/device support: WMNs are more scalable because of its heterogeneous network/ device support also called it as interoperability and integration features in WMNs. However, the existing security mechanisms do not consider these two essential features in their mechanisms. As a result, this feature is more vulnerable to various attacks.

Three-level hierarchy: WMNs follow the three level hierarchies: gateway level, router level and client level which is shown in Figure 1. In this three level hierarchy WMNs are more scalable and easy to

maintain than any other wireless networks. Existing security mechanisms works on either router level or client level. Hence, WMNs three-level hierarchy is vulnerable to diffident type of attacks.

Decentralized authentication: In WMNs, gateways authenticate the mesh routers and routers authenticate mesh clients. Here, authenticationprocess has taken distributive at gateways as well as routers. Decentralized authentication of WMNs nodes always scalable and can avoid single point of failures.

In SSF, design we use conventional IPsec to authenticate gateways [14]. IPsec mainly operates two modes: transport mode (host to host) and tunnel mode (gateway to gateway), we use tunnel mode in SSF. Tunnel mode provides security association between gateways in which internet key exchange (IKE) has been taken place by using diffi-hall men algorithm. These keys are used to provide authentication, confidentiality for gateways.

Each router in the mesh network is authenticated by its own public key, which is chosen from elliptic curve cryptography (ECC) [4]. ECC devices require less storage, less power, less memory, and less bandwidth than other systems. Moreover, it takes less time in the authentication verification process and more efficient than RSA. For example, to achieve the security level of a 1024-bit RSA cryptosystem, ECC requires only 160-bit key length. To create message digest we use SHA-1 algorithm.

3. RELATED WORK

Deployment of wireless mesh networks is very much required due to its unique features associated with any wireless or wired networks. However, the unique features are severely affected by various attackers. We have studied existing security mechanisms to protect these features. We also compare the existing security frameworks with five aspects in the following:

Yahchao Atypical has proposed *ARSA* for multihop WMN [1]. ARSA security framework consists of two levels: Backbone Mesh, Client Mesh in ARSA. Id Based Cryptography (IBC) is used to authenticate backbone mesh, as well as client mesh. In each node certification process, communication and computational overhead can be reduced because this security framework follows IBC instead of X.509 certification. To provide the operator service, each operator (O_i) needs to authenticate each mesh client (C_{ij}) by broker $B_{i,}$ and mesh router (R_{ij}) by session key (K_{ij}). Second, (O_i) issues the temporary keys when each (C_{ij}) needs operator service. In the above mentioned five aspects, it supports client multihop communication, but no multihop communication support on backbone network. In addition, it does not support heterogeneous networks/device and no communication between different operators. As a result, ARSA security framework is not scalable in WMNs. Colluding attack can be prevented at client mesh. When a mesh client needs to send an authentication request to router (R_{ij}), if mesh client is not within the radio range of (R_{ij}), then it increase the communication range to establish a direct communication between access point/ router and mobile node. This type of authentication process increases the number packet collisions in client mesh network.

An *Adaptive key management framework* has developed by Mi Wen et al [10]. This framework is mainly designed for wireless mesh and sensor network security. MPKM, MGKM, and TKM protocols are used to distribute the keys among sensor and mesh networks. Out of three protocols Matrix Based Pairwise key Management (MPKM) protocol is essential to handle pairwise key establishment for the resource limited sensor nodes. Here, Base Station (BS) is acting as a trusted server and issues the seed (s_i) value to the group head and creates row seed matrix D based on prime number q, creates column seed matrix B based on GF(q). The matrix *B* is public while the matrix *D* is kept secret by the base station. Since *D* was symmetric, the key matrix $K = AB$ can be written as:

$$K = (DB)^{T}B = B^{T} D^{T}B = B^{T} DB = (AB)^{T} = K_{T}$$

Thus *K* is also a symmetric matrix and $K_{ij}=K_{ji}$, where K_{ij} is the element of *K* at i^{th} row and j^{th} column. K_{ij} (or) K_{ji} is the pairwise key between node N_i and node N_j. The same technique is used to derive Matrix Based Group Key (MGKM) among cluster heads. In Threshold Key Management (TKM), the group keys of the WSNs will be calculated as a secret key shared by *n* mesh nodes. The secret key can be recovered by a coalition of *t* mesh nodes. MPKM and MGKM protocols are mainly depends on BS seed values if this seed value is hacked by attacker, then all sensor nodes belongs to this BS are vulnerable. Moreover if numbers of sensor nodes are more, computing pairwise secret key takes more time due to number of columns and rows are more. Hence, adaptive key management framework is not scalable.

Mobisec framework is a centralized secure backbone framework [3] . Key Server (KS) issues the keys to the newly joining routers. Once new router acquires of its private key, then it starts sending join request. Whenever this request packet is received by its authenticated neighborhood routers, first check the authentication of the packet. If it is valid then this packet broadcast into the network. This process has been continued until it reaches to the KS. When KS receives this request, first it authenticate by private key, which

is issued at joining time. If this authentication is valid then the KS forwards secure communication key encrypted with private key to the request-initiated router. To prevent stale packets authentication replay attack, this secure communication key is periodically updated. This process creates additional communication and computational overhead. Mobisec framework is not scalable due to the entire process is failed once the centralized key server is down. Furthermore, it does not support heterogeneous networks and colluding attacks are still possible.

DSA-Mesh is an enhanced version of Mobisec, it could overcome the scalability problem at backbone by introducing distributed security architecture [2]. Here, backbone nodes (routers) divided into two groups: generic nodes and core nodes. This architecture mainly works on distributed proactive request protocol, and Session Secret agreement protocol. In distributed proactive request protocol, initially any generic node M_i broadcasts the authentication message. When this packet is received by core nodes, first verify the M_i certificate. Then is reply back to the M_i with it K_i. M_i wait until it receives the t replays, then it forms the group key with t^{th} reply. Eventually it verifies the resultant key with known public key K_k. If this key is valid, it can be used to obtain the next session secret S and valid t_s seconds. This mechanism has problems such as each M_i gets only t-1 response it does not construct the public key.

Second, Session Secret Agreement Protocol in which key exchange mainly has taken place among core node. Initially all core nodes selects peer master of the session. Peer master broadcast a message. When a core node receives the message it verifies the authentication and authorization. Then, it chooses a random number sap mod p reply to peer master. M_i waits for the n-1 replies, and after verification of message integrity and sender's identity; it sends the last message to all core nodes. For each received message, M_i A. Eventually A derives the public key and broadcast among core nodes. For each k_p session expire or one of the core node fails, all core nodes have to choose one peer master, It creates extra overhead. Moreover, all core nodes should maintain their updated information whether node alive or not. Hence, this mechanism is not suitable for large-network.

SeGroM framework has proposed by Jing Dong [6]. The main objective of this framework is to reduce the communication and computation overhead of secure group communication. To achieve this, SeGroM-Hop was developed, in which each head members of the group, encrypt the secret key (Kd) with each hop key of their downstream members instead of both upstream and downstream members. This Kd values prevents loss of forward and backward secrecy of each data packet. SeGrom framework is not discussed security of multihop client mesh, and heterogeneous networks. Moreover, it works only on single group communication not for multiple group communication. Moreover, if the group head is compromised the entire network communication control by an attacker.

802.11s: 802.11s is a standard for wireless mesh network certified by Task Group (TG) in 2006 [8]. The security framework of 802.11s supports cryptographic functionalities authentication, integration, confidentiality. To justify these functionalities, 802.11s framework is organized hierarchically: authentication server (AS), mesh key distributor (MKD) at upper level, Mesh Authenticator (MA), Mesh Point (MP) at lower level. Here, the mesh node hierarchy changes based on security keys it holds, if the MP has both MKD, MA functionalities it is called portal or gateway, else if MP has neither MKD nor MA then it called as supplicant. In the process of mesh point authentication, Authentication Server (AS) derives Pair-wise Master Key (PMK) for MKD by using Pre-Shared Key either (PSK) or master session key (MSK) then MKD derivers PSK-MA for mesh authenticator (MA). Eventually, MA derives a Pairwise Transient Key(PTK) for supplicant (MP) using PSK-MA. 802.11s only supports two level authentication and also not consider the heterogeneous networks/device support. Two level authentication of 802.11s have problems while selecting the precise mesh key distributor (MKD) among mobile points (MP) and selecting message authenticator (MA) are still an ambiguous process. Moreover, it is not addressed decentralized authentication.

IEEE 802.16j-2009 Multi-Hop Relay Security Architecture: Distributed 802.16j standard follows three level hierarchies [5]. Top-level master Base Station (BS) authenticates all two level hierarchy nodes called Relay Station (RS) and Mobile Station (MS). Initially these RS is formed Security Association (SA) with BS. Once MS sends authentication request to RS, it forms security association with MS and then RS forward to next subordinate RS, if the BS is not within the rage. The subordinate RS then establish SA with MS. This process will continue until request reaches to base-station. If the master base-station captures, the entire system will be under attacker control. Moreover, it suffers from another security issues, for example, if a MM sends wrong request, it has to forward by intermediate RS until master BS recognizes the fraud id MM, means all the RS and SA association process had taken place before it is wasted. It supports heterogeneous devices communication but not the heterogeneous networks. This framework cannot be adapted to ad-hoc and sensor networks due to its high Communication and computational overhead.

Analytical study of security frameworks with respective all five different scalable features of WMNs results are shown in table 1. Base on results we have identified, existing security frameworks are

inadequate to support all the five features which are useful for grater scalability of WMNs. Table 1. shows that comparison of all above mechanisms:

Table 1. Comparison of security mechanisms vs scalable feature of WMN

	ARSA	MobiSec	DSA-Mesh	AKM in WMSN	802.11s	SeGroM	802.16j
Protect against Unauthorized nodes	YES	YES	YES	YES	YES	YES	YES
Protect against Colluding attack	NO	NO	NO	NO	NO	NO	NO
Three level Hierarchical Infrastructure	YES	No	NO	YES	NO	NO	YES
Decentralized authority	YES	NO	YES	NO	NO	NO	YES
Heterogeneous network support	NO	NO	NO	NO	NO	NO	NO

4. DESIGN OF SCALABLE SECURE FRAMEWORK (SSF) ARCHITECTURE

Since WMNs were lacked the attack resilient security frameworks, unique features of WMNs are more vulnerable to various attacks. To secure these features we have designed a Scalable Secure Framework (SSF) for WMN. SSF main objectives are to protect against internal and external attacks, decentralized authentication and supports heterogeneous networks (two different client mesh networks). Figure 2. depicts the wireless mesh networks three level architecture. Gateways are placed at top level and these nodes are stable nodes. Routers have less mobility and these nodes are authorized by gateway nodes. Third level nodes are mesh clients and these nodes have high mobility. To sustain heterogeneous network/device support, we consider two different client mesh networks: 802.11s and Wi-Fi network. Moreover, to maintain the distributive nature all three level nodes are distributed in the network.

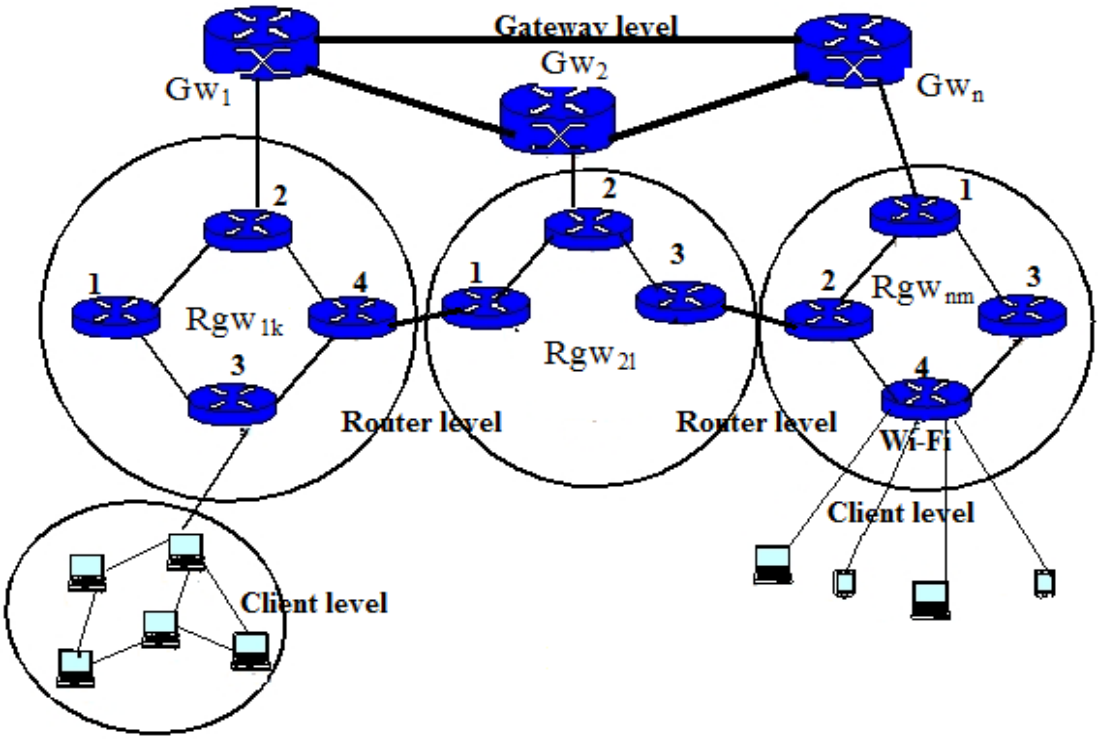

Figure 2. Example of Three level hierarchy of Wireless mesh networks

Secure Scalable Framework (SSF) has designed to secure all five the scalable features of WMNs. In SSF, each gateway provides authentication, integrity, confidentiality, and non-reputation for every backbone router authentication. Gateways are authenticated by conventional IPsec tunnel modes that provide more secure authentication among gateways. Router authentication is done when any router join or leave from the network. We also consider two different networks 802.11s and Wi-Fi as a client mesh network to provide client authentication [Wankhedep.g. 2012]. SSP follows the Table 2. notations. SSF design consists of three level authentication: Gateway level, router level, client level.

Table 2. SSP notations

Gw_i	level one node (gateways)
Gwp_i && Gwq_i	public and private keys of Gw_i
M_{gwsig}	Message singed by Gw
Rgw_{ik}	k^{th} number of router belongs to Gw_i
K_{id}	router key identifier
$Krgw_{ik}$	Shared key between Rgw_{ik} and Gw_i
$T_{Rgw_{ik}}$	expiration time of K_{id} of Rgw_{ik}
$Rgwp_{ik}$ & $Rgwq_{ik}$	Public and private keys of Rgw_{ik}
$AReq_{Rgw_{ik}}$	authentication request of Rgw_{ik}
$ARep_{gw_{ik}}$	Authentication replay by Gw_i
$H(M)_{Krgw_{ij}}$	Message digest created by Rgw_{ij}
$Rgwn_{ij}$	Neighboring router in Gw_i set
$DAReq_{gw_{il}}$	Deauthentication Request

4.1 SSF authentication process at Gateway level

SSF supports distributed Gateway's (Gw_i's) communication. This communication supports WMN to increase the scalabily in greater extantion. Here, the Gw_i's are connected to each other through a wired network and follow conventional IPsec tunnel mechanisms to securely communicate any two Gw_i. In which Gw_i's derives mutual authentication keys (Gwp_i). Then Gw_i's use the authentication keys exchange their authenticated routes Rgw_{ik}'s information along with their Gwp_i. Authenticated Gw_i's forward the authentication requests of other Gwi routers to get authenticate by correspoing Gw_i. This process increases the security interms of colluding attacks in backbone mesh.

4.2 SSF authentication process at router level

Authentication of Rgw_{ik} is more important and critical due to multihop backbone mesh, wireless interference and colluding attackers. In SSF, we design router authentication and deauthentication processes in two different algorithms. Algorithm 1. considers the router Rgw_{ik} authentication process.

When a new router (Rgw_{ik}) request with key(k_{id}) to join in gateway (Gw_i). Gw_i verifies key (k_{id}) with valid router ids. If it is valid then it issues message (M_{gwsig}) consists of key (k_{id}) and expiration time (T_{Rgw}) signed by its private key (Gwq_{ik}) and session key ($Krgw_{ik}$) to router (Rgw_{ik}). Once Rgw_{ik} is placed in the network, it generates its own public key ($Rgwp_{ik}$) by using elliptic curve cryptography then creates an authentication request. This request contains the following fields $\{M_{gwsig},\{k_{id},T\},Rgwp_{ik},H(M)\}$ which is a message digest of whole message created by session the key $H(M)=\{M_{gwsig},\{k_{id},T\},Rgwp_{ik}\}$. Router ($Rgw_{ik}$) disseminates authentication request.

When this request is received by neighboring nodes ($Rgwn_{ij}$), then decrypt message (M_{gwsig}) with gateway public key (Gwp_i) and verify k_{id} and T. If it is valid then node stores k_{id} and then authentication request disseminated by $Rgwn_{ij}$. Otherwise this request is dropped from $Rgwn_{ij}$'s. This process continues until it reaches to Gw_i. If this request is received by nighbouring router which does not belongs to Gw_i, then it verifies T for particular k_{id}. If it is valid then send a request message for Gwp_i. Router (Rgw_{ik}) responds to this request with Gwp_i key. Once neighbor receives, Gwp_i then verifies M_{gwsig} and forwards to Gw_t for further verification. When the valid verification reply comes from gateway (Gw_t) then nigbouring node starts the communication with Rgw_{ik}. If Gw_i receives the authentication request then it verifies M_{gwsig} by its public key. If it is valid then creating message digest of whole message H'(M) by the session key. The two message digests H(M) and H'(M) values are same then Gw_i stores($Rgwp_{ik}$) in its memory and create replay which contains { k_{id}, time, public key}values are signed by its private key and sends reply through all node disjoint paths to overcome the colluding attacks. When the neighbor receives this replay first this message is decrypted by known gateway public key (Gwp_i). If is valid then router ($Rgwp_{ik}$) appended to corresponding k_{id} in its information table. It forwards next router, this process will repeat until it reaches to Rgw_{ik}. Eventually, all the backbone routers authenticate $Rgwp_{ik}$ and it can be used for all secure data communication.The following algorithm depicts when a router join or leaves from the network.

Algorithm 2 considers the router (Rgw_{il}) deauthentication process. Any router (Rgw_{il}) wants to leave from the network, it creates deauthentication message (DAReq) which consists of TTL value of DAReq, kid, $Rgwp_{ik}$, DAid all these are values signed by $Rgwq_i$ to Gwi. DAReq message is sent through all node disjoint paths. When this message is received by neighbouring hops, it decrypts this message by Rgw_{il} public key. If it is valid then it forward to next router in the node disjoint path. Gw_i verifies DAReq if it is valid then remove Rgw_{il} public key and disseminates message to all Gw nodes. Eventually, GRw_{il} completely is isolated from backbone network.

Storage Overhead: In SSF router level, each router (Rgw_{ik}) need not stores all the public keys of backbone routers. Instead of this, each router (Rgw_{ik}) stores authenticated routers (Rgw_i's) public keys ($Rgwp_i$) and its represents with P_K and stores the gateway public key (Gwp_i) a particular gateway (Gw_i). In addition router (Rgw_{ik}) stores the bridging nodes (e.g. ($Rgw_{17,}$ Rgw_{23})) authenticated public keys which are represented by P_B. The total number of storage overhead of each router is P_K + P_B+ one gateway public key (Gwp_i).

Communication overhead: When the neighboring node receives the authentication request, it does not verify the entire authentication request message. Router has to check only the authentication of the received request by gateways public key and TTL value. Routers need not check the integrity of the packet, which is verified only at gateway.

Algorithm 1. Router (Rgw_{ik}) authentication Process

When the new node Rgw_{ik} sends a join request with k_{id} to Gw_i
Gw_i disseminates k_{id} to all Gw nodes
Gw_i issues M_{gwsig}, $Krgw_{ik}$, to Rgw_{ik}
Rgw_{ik} generates its own public and private keys $Rgwp_{ik}$, $Rgwq_{ik}$
Rgw_{ik} create and disseminates authentication request $AReq_{Rgw_{ik}}$
$AReq_{Rgw_{ik}}$ is Received by its neighbours $Rgwn_{nj}$
If $Rgwn_{nj} \in Gw_i$
Extract M_{gwsig} from $AReq_{Rgw_{ik}}$
If $T_{Rgw_{ik}}$ & Gw_i authentication = valid
Store K_{id} & Broadcast $AReq_{Rgw_{ik}}$
Else
Drop $AReq_{Rgw_{ik}}$
If $Rgwn_{nj} \notin Gw_i$
Send a request to Rgw_{ik} for Gwp_i
Rgw_{ik} replies to $Rgwn_{nj}$
If $T_{Rgw_{ik}}$ && Gw_i authentication = valid
Store K_{id} & Forward $AReq_{Rgw_{ik}}$ to Gw_t
Else
Drop $AReq_{Rgw_{ik}}$
If Gw_i receives $AReq_{Rgw_{ik}}$
If $T_{Rgw_{ik}}$ && Gw_i authentication = Valid
If $H'(M)_{Krgw_{ik}} = H(M)_{Krgw_{ik}}$
flag = 1
Store the public key and drop $Krgw_{ik}$
Gw_i creates authentication reply ($ARep_{gw_{ik}}$)
$ARep_{gw_{ik}}$ Forward to Rgw_{ik} by all node disjoint paths
Gw_i disseminates $Rgwp_{ik}$ to all Gw nodes
Else if flag =0
Drop $AReq_{Rgw_{ik}}$

Algorithm 2. Router (Rgw_{il}) deauthentication process

Rgw_{il} sends request a deauthentication request ($DARep_{gw_{il}}$)
singned by $Rgwq_{il}$ Through all available node dijiontpaths to Gw_i
$DAReq_{Rgw_{ik}}$ Received by its neighbours $Rgwn_{nj} \| Gw_i$
decrypt $DAReq_{Rgw_{ik}}$ with $Rgwp_{il}$
If $T_{Rgw_{il}}$ & Rgw_{il} authentication = Valid & $Rgwn_{nj}$
Forward $DAReq_{Rgw_{ik}}$ to Gw_i
Gw_i remove $Rgwp_{il}$ key from the network by sending to all Gw nodes

4.3 SSF authentication process at mesh client

SSF supports two types of client mesh networks: 802.11s mesh and Wi-Fi. 802.11s provides multi-hop communication and Wi-Fi provides single hop communication. We have studied 802.11s with respect to all five features of WMN. When it works on client mesh, it has problems such as selecting the precise mesh key distributor (MKD) among Mobile Points (MP) does not clarify and selecting message authenticator (MA) is still an ambiguous process. To overcome the ambiguity problems of 802.11s, SSF has fixed MKD for a particular network. In Figure 2, Rgw_{15} acts as a key distributer for all mesh clients in 802.11s. Message authenticator (MA) is selected from any two mesh clients based on first come first sever. If two mesh clients are new then the mesh client which is nearer (less hop_count) to MKD selected as MA.

SSF consider one more network called Wi-Fi network. Wi-Fi is a one hop communication network and secured by Wi-Fi Protected Access (WPA2). WPA2 suffers from authentication flooding and (RTS/CTS) flooding. To overcome this problem, mesh router (Rgw_{n6}) sets the threshold value to control the flooding of authentication and RTS/CTS packets of mesh clients.

5 SECURITY ANALYSIS

Colluding attackers: Colluding attackers (except router Rgw_{14} all Gw_1 routers) intention is to isolate target (legitimate) node (Rgw_{14}) by stop sending its authentication requests [16] shown in Figure 2. In existing frameworks, target node (Rgw_{17}) is not authenticated by Gw_1 due to Rgw_{11}, Rgw_{12},Rgw_{13} in Gw_1 are colluding attackers. These attacks drop all received authentication requests of Rgw_{14}. Hence, Rgw_{14} is not authenticated by Gw1. SSF this problem is overcome by supporting multiple gateways and broadcast the authentication request. In SSF, colluding attackers are inadequate to stop the authentication requests because Gateway (Gw_1) is integrated with other gateways in the network. All the bridging routers/gateways forward the authentication request to the actual gateways. When router Rgw_{14} broadcast the authentication request is received by all colluding routers of Gw1 and router Rgw_{21} of Gw_2. Rgw_{21}forward this request to the Gw_2.Then Gw_2 forward this authentication request to Gw_1.

Imprinting attack: The mechanism by which devices acquire the self-signed mediator's certificate is called imprinting. In WMN, any mesh client can join or leave at any time. When a new node wants to join in client mesh network or infrastructure mesh, it sends authentication request to the access point or gateway. Once it is received by AP/gateway, it issues the key to the new node. The new node always selects the owner, which issues the key first. In this process, attacker takes an advantage by issuing the key to the new node before the AP/GATEWAY. This attack often disturbs the multihop networks (supports multihop communication).To isolate imprinting attackin SSF, each router (Rgw_{il}) / mesh client (MC) knows the authenticated AP/GATEWAY public key before join in the network.

Replay attack: The attacker records the two legitimate nodes authentication messages that is nothing but a passive eavesdropping attack. Then the attacker comes into active phase and replays recorded message to one of the nodes attempting to impersonate as a previous legitimate user. This attack is overcome by SSF because every authentication packet has TTL value. This value is invalid once it reaches to Gw and any neighboring node does not accept different authentication requests with same TTL values of router (Rgw_{il}).

Node Deprivation attack: The attacker gets the deauthentication request from when the router (Rgw_{il}) authenticate from the network. If router (Rgw_{il}) re-enters with same id then attacker often sends deauthenticated message to authentication server to prevent the legitimate node from the network access. The justification to prevent this attack is same as replay attack.

6 CONCLUSION

In this paper, we have studied existing security frameworks with respect to five different scalable features of wireless mesh networks. Based on the study we identified security framework are inadequate to support all the features. We designed Scalable Secure Framework (SSF) for WMN by supporting all scalable features. SSFsecure all scalable features in three levels: gateway level, router level and mesh client level by using robust three level authentication mechanisms. Security analysis proves that, SSF secures the node when it joins or leaves from in the hierarchical WMNs.

REFERENCES

[1] Yanchao Zhang, ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks. IEEE Journal on Selected Areas in Communications 24(10): 1916-1928 (2006).

[2] Martignon .F, S. Paris and A. (2008) Capone DSA-Mesh: a Distributed Security Architecture for Wireless Mesh Networks SECURITY AND COMMUNICATION NETWORKS in Wiley InterScience, pp. 1-17.

[3] Martignon .F (2008) MobiSEC: A Novel Security Architecture for Wireless Mesh Networks Q2SWinet'08, October, pp. 35-42.
[4] Zhang.Y. (2008). Security in Wireless Mesh Networks. CRC Press.
[5] 802.16j (2009) - IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment 1: Multiple Relay Specification , E-ISBN : 978-0-7381-5921-8 June 12 2009.
[6] Dong .J, Ackermann .K and Nita-Rotaru .C, (2009) "Secure Group Communication in Wireless Mesh Networks," Ad Hoc Networks, Vol. 10, No. 16 , pp. 1563-1576.
[7] Muhammad.S and Choong.S. (2009) Security issues in wireless mesh networks. In IEEE/IPSJ International Symposium on Applications and the Internet, pp. 717-722.
[8] Shariful.Md and Abdul Hamid. (2009) Shwmp:a secure hybrid wireless mesh protocol for ieee802.11s wireless mesh networks. Springer-Verlag Berlin Heidelberg, pp. 95-114.
[9] Ping.Y and Yue.W. (2010) A survey on security in wireless mesh networs. IETE TECHINICAL REVIEW, vol.27: pp. 6-14, JAN-FEB.
[10] Mi Wen1, Zhi Yin. (2010) An Adaptive Key Management Framework for the Wireless Mesh and Sensor Networks Wireless Sensor Network, 2,pp. 689-697.
[11] Ganesh,.K., Khilar.P(2010) :Routing misbehavior detection and reaction in MANETs, ICIIS,2010International Conference on July pp. 80-85.
[12] AL-Sakib khan. (2010). security of self-organizing networks, MANET, WSN, WMN, VANET CRC Press.
[13] Wi-Fi Alliance article (2003) Wi-Fi protected access: strong, standards-based, interoperable security for today's Wi-Fi networks. Wi-Fi Alliance, Apr 2003.
[14] Davis, Carlton R.(2001), "Ipsec: Securing Vpns " McGraw-Hill Professional, ISBN:l0072127570.
[15] Wankhede p.g. and Chavhan k.l (2012): Wireless mesh network securities, BIOINFO Secu-rity Informatics Volume 2, Issue 2, 2012, pp.-45-48.
[16] K. Ganesh Reddy and P. Santhi Thilagam (2012), "Taxonomy of Network Layer Attacks in Wireless Mesh Networks", In the Proc. of Advances in Computer Science , Engineering and Applications, AISC 167/2012, Springer Verlag, pages: 927-935.
[17] Redwan.H, Ki-Hyung.K, Survey of security requirements, attacks and network integration in wireless mesh networks, Frontier of Computer Science and Technology 2 (2008) 3-9.
[18] Sahil.S, Anil.G, Current state of art research issues and challenges in wireless mesh networks, in: IEEE Second International conference on computer Engineering and Applications, 2006, pp. 1-17.

BIOGRAPHY OF AUTHORS

K. Ganesh Reddy received the B.Tech in degree in Information Technology from Andhra University, Andhra Pradesh and M.Tech in Information Security from National Institute of Technology Rourkela, Orissa India in 2007 and 2010. He is currently studying at National Institute of Technology at surathkal, India as a Ph.D student. His area of research is security in wireless Ad-hoc and mesh networks.

P. Santhi Thilagam received her Bachelor degree in Computer Science and Engineering in 1991 and Master degree in Computer Science and Engineering in 2000 from College of Engineering, Guindy, Anna University, Chennai, India. She is currently working as a Associate Professor in the Department of Computer Science & Engineering, National Institute of Technology Karnataka, Surathkal, India. She has published more than 15 papers in International journals and more than 30 papers in International conferences. Her research interests are mainly in the areas of Distributed Data Management, Database mining and Social Network Analysis.