A Secure Authentication Scheme in Multi-operator Domain (SAMD) for Wireless Mesh Network

Ninni Singh, Gunjan Chhabra, Kamal Preet Singh and Hemraj Saini

Abstract Wireless mesh network (WMN) is considered to be an evolving technique because of self-configuration and adaptive features, it supports large-scale network especially in an organization and academics. As with any network, communication among nodes plays an important role, when two nodes in a network communicate with each other via the Internet, secure authentication is an imperative challenge. In literature, there are many approaches that have been suggested to deliver a secure authentication between nodes in wireless mesh network (WMN), however, all these outlines contain some disadvantages, i.e. management cost of the public key and system complexity. Our suggested proposed approach is dealing with one of the wireless mesh network challenges, i.e. Mutual authentication. Here in this we have considered the three authentication techniques, i.e. Inter-, Intra- and Inter-Operator domain authentication. SAMD (**Secure Authentication Scheme in Multi-Operator Domain**) hides the location, communication path and network access and apart from that it will resist to the adversary, key forgery and modification attack. As a result, we have assessed the performance of the proposed design in terms of Authentication cost, Encryption cost, Key validation, Key Generation, Throughput and System Delay, which indicates our scheme more efficient than other schemes. Results show that it will efficiently work in real-time traffic.

Ninni Singh (✉) · Gunjan Chhabra · K.P. Singh
Department of Centre of Information Technology, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India
e-mail: ninnisingh1991@gmail.com

Gunjan Chhabra
e-mail: g_chhabra@yahoo.com

K.P. Singh
e-mail: kamalpreet1010@gmail.com

Hemraj Saini
Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, India
e-mail: hemraj1977@yahoo.co.in

S.C. Satapathy et al. (eds.), *Proceedings of the International Conference on Data Engineering and Communication Technology*, Advances in Intelligent Systems and Computing 468, DOI 10.1007/978-981-10-1675-2_35

Keywords Multi-operator · Inter-Domain · Intra-Domain · Inter-Operator · Wireless mesh network

1 Introduction

The Wireless Mesh Network is an emerging technology, its fast, inexpensive network deployment, easy Internet connectivity features makes it a popular choice for Wireless ISP (Internet Service Provider). WMN represents the combination of wide area cellular network and high-speed Wi-Fi networks. Nevertheless, without any security in WMN, it is impossible to securely exchange any information [1, 2]. Various research work is in progress. At present there are no formal methods to authenticate the network in WMN. Security is an open challenge in WMN. In recent times lot of research work is in progress. (Santhanam) [3] Proposed an authentication scheme grounded on Merkle tree. There whole consideration is to authenticate the client irrespective of the entire security architecture and mesh client roaming. (Fu et al.) [4] Proposed an authentication scheme in which he integrate various existing techniques, i.e. Virtual certificate authority, zone-based hierarchical structure and multi-signature scheme. (Zhang et al.) [5] Proposed an architecture, in which, if mesh client wishes to roam to another network, then it requires a pass from trusted third party. In this paper, we have proposed a novel secure authentication scheme for multi-operator domain. This is the extended version of [6] paper. The proposed technique is a broker-based three-tier hierarchical architectures. The broker is a reliable third party which lives in the first tier. Broker consist of a private key generator, whose function is to generate a private key. Gateway lives in the second tier and router lives in the third tier. Both gateways as well as router are considered as a trustworthy node because of their less mobility. Any node willing to enter into the network, it has to submit its own identity (identity of any node act as the public key of that node) to the broker and broker hand over private key (by giving identity as an input to the private key generator) to that node. If the newly entered node is the router or gateway, instead of private key it can also send a ticket and its own signing rights to them. Now onwards both gateway and router possess the same functionality of the broker. This technique is formally verified on AVISPA SPAN, which shows that there is no attack is possible and private key is not forgeable. SAWMN (Secure Authentication in Wireless Mesh Network) reduces the overall system complexity by not explicitly managing the public keys and it also efficiently works in real-time environment. Our suggested proposed approach extend above discussed technique to accomplish the authentication procedure in Inter-domain and Intra-domain. As a result, we have assessed the performance of the proposed design in terms of security analysis, which indicates our scheme more efficient than other schemes. The rest of the paper is structured into the following categories: in section second we discuss the related works. In section third we have elaborated the proposed technique (SAWMN) and Inter- and

Intra-domain Authentication. In section four we have shown the simulated results and finally in section five we conclude our paper.

2 Related Work

For secure communication among nodes, there will be a demand of some authentication mechanism in a wireless network. Many researchers are working on this area, few of them, we will discuss in this section. Authentication among nodes can be attained, when any two nodes present in the network, Inter-domain (mesh clients roam from one operator domain to other operator domain), Intra-domain (mesh clients roam within a same domain operator) and Intra operator (mesh client roams from one domain to another domain within same operator). (Summit R.) [1] Proposed a token-based authentication scheme, in which token is utilized for verification purpose. Token works same as that of digital signatures by integrating public key with subjects ID and it also verifies the authenticity of subject ID in the issuer realm. This protocol reduces the time required for authentication and also somehow restricts the communication between the home network to the roam or foreign network, but it requires a roaming credential that will be shared among servers and this incurs some cost for supervision. (Ford) [2] Proposed a key agreement protocol based in identity-based encryption technique. This scheme overcomes the above discussed problems, i.e. the administration cost. One of the biggest drawbacks of this scheme is that it cannot guard the user's privacy. (Yeh and Sun) [3] Proposed a four-party password-based authentication technique and key establishment protocol. To accomplish all this feature, there will be a requirement of public key infrastructure for the distribution and confirmation of server's public key to the clients. But the problem with this approach is that it is not well suited for lightweight computing domain. (Ren-Junn) [4] Proposed an authentication schemes, which utilizes symmetric encryption technique and hash function.

(Hung-Yu Chien) [5] Proposed an authentication scheme, which utilizes a public key encryption technique. Instead of using certificates, they utilize hash function, which decreases the management cost of certificates. To accomplish this feature additional server is required, which somehow increases the time delay. All the above discussed schemes incur some drawbacks either in terms of time delay in computation, authentication cost, having high storage cost and system complexity. In our proposed authentication technique, we work on these drawbacks. Proposed scheme reduces the authentication cost, system complexity, power consumption and timing cost, and also shows the comparative study with respect to the traditional authentication technique used in wireless mesh network.

3 Proposed Technique

In the former section we have discussed various research works of different authors. Now in this section we have elaborated the extended version of [6]. In this [6] paper we have discussed the key management in the proposed architecture. The proposed technique is a broker-based three-tier hierarchical architectures. The broker is a reliable third party which lives in the first tier. Broker consist of a private key generator, whose function is to generate a private key. Gateway lives in the second tier and router lives in the third tier. Both gateways as well as router are considered as a trustworthy node because of their less mobility. Any node willing to enter into the network, it has to submit its Own identity [7] (identity of any node act as the public key of that node) to the broker and broker hand over private key (By giving identity as an input to the private key generator) to that node. If the newly entered node is the router or gateway, instead of private key it can also send a ticket and its own signing rights to them. Now onwards both gateway and router possess the same functionality of the broker [8, 9]. This technique is formally verified on AVISPA SPAN, which shows that there is no attack is possible and private key is not forgeable. SAWMN reduces the overall system complexity by not explicitly managing the public keys and it also efficiently works in real-time environment (Fig. 1).

Our suggested proposed approach extend above discussed technique in order to accomplish the authentication procedure in Inter-domain [10] and Intra-domain. Here we used one additional server named as Main server, which contain the all related information like IP address of the sub-module, roaming information, etc.

Main server performs various functionality, like if any mesh client roams from one domain to some other domain, then this activity is first noticed by main server, which internal hand over the mesh client IP address of the foreign domain. After this foreign domain performs some authentication process between mesh clients and mesh router.

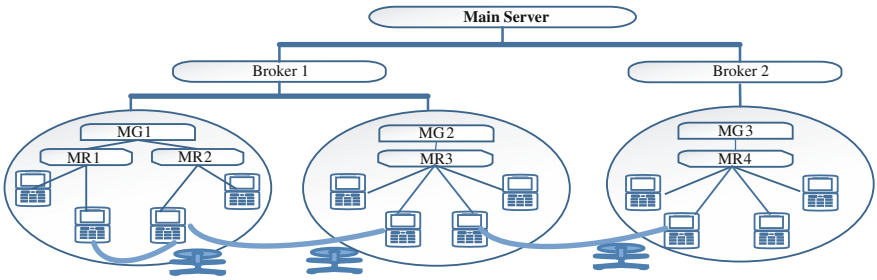

Fig. 1 Block diagram of authentication network

3.1 Inter-Domain Authentication

When mesh client roams from broker 2 domains to broker 1, Inter-domain authentication has been taking place between the mesh router and the mesh client. Following an authentication process will be followed by MC and MR_1.

$$(1) \quad MR_1 \rightarrow MC: = TK_{MR_1}^{B_1 MG_1} = \{\text{Exp}, ID_{B1}, t_{B1}, ID_{MG1}, ID_{MR1}, \text{Sig}(\text{gateway } 1)\}.$$

$$(2) \quad MC \rightarrow MR_1: = TK_{MC}^{B2} = \{\text{Exp}^{!}, ID_{B2}, t_{B2}, ID_{MC}, \text{Sig}(\text{broker } B2)\}.$$

$$(3) \quad MR_2 \rightarrow MC: = TK_{MC}^{MR_1 MG_1} = \{\text{Exp}^{!}, ID_{MG1}, ID_{MR1}, ID_{MC}, \text{Sig}(\text{Mesh router1}) t_1, N_1\}.$$

$$(4) \quad MC \rightarrow MR_1: = \{t_2, N_2\}.$$

The mesh router periodically broadcasts message 1 to its coverage area. When mesh client roams from broker 2 to broker1 called inter-domain. After receiving message 1 following operations are performed (Fig. 2).

1. It first checks the freshness of the Expiration or validity of the ticket.
2. Retrieve broker 1 public key and from broker's public key, it verifies the signature of gateway 1.
3. After verification, it computes the shared key $K_{MC--MR1} = \text{e}(ID_{MC}, ID_{MR1})$, where $= ID_{MR1} = \text{H1}(\text{Exp, IDMG1})$.

Mesh client now sends a message (2) to mesh router 1. After receiving the message (2) it performs following tasks.

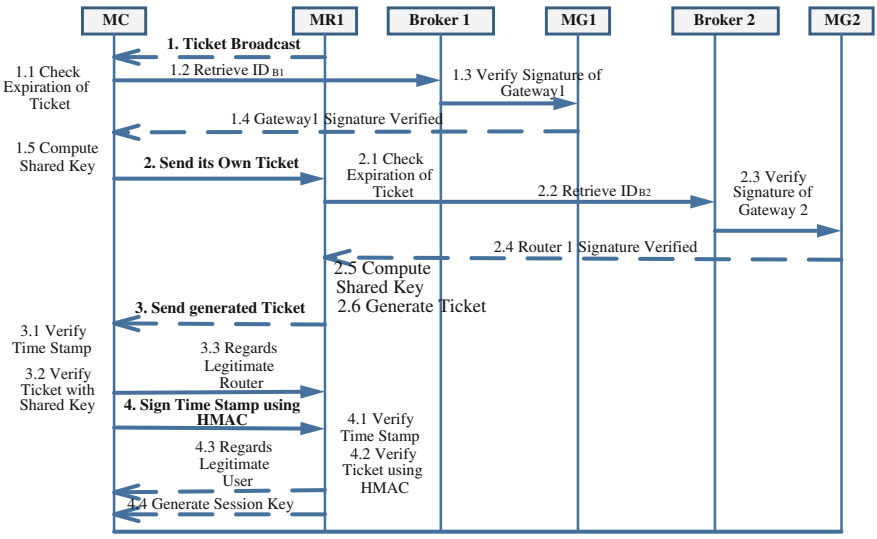

Fig. 2 Inter-Domain authentication

1. Check for the expiry date on the Client ticket and make certain that it is not expired.
2. Retrieve broker 2 public key and from broker's public key, it verifies the signature of gateway 2.
3. After verification, it computes the shared key $K_{MR1--MC} = \mathrm{e}\ (ID_{MR1}, ID_{MC})$.
4. Mesh router 1 generates tickets for newly entered nodes, i.e. Mesh client.

$$TK_{MC}^{MR_1MG_1} = \{\mathrm{Exp}^{!}, ID_{MG1}, ID_{MR1}, ID_{MC}, \mathrm{Sig}(\text{Mesh router1})t_1, N_1\}.$$

5. Before sending to the mesh client, mesh router 1 sign the ticket with HMAC, $1 = TK_{MC}^{MR_1MG_1}$.

Mesh router 1 now sends a message (3) to mesh client. After receiving the message (3) it performs following operations.

1. Check the newness of timestamp and the expiry of the ticket.
2. Verify the ticket $TK_{MC}^{MR_1MG_1}$ Using shared key $K_{MC--MR1}$ (Computed by mesh client).
3. If the verification of ticket is done successfully, then mesh router is considered as an authentic router or trustable router.
4. Generate a timestamp and create a signature on it, by signing it with the shared key $(K_{MC--MR1})$.

Mesh client now sends a message (4) to mesh router 1, after receiving a message (4) it perform the following operations.

1. Check the newness of timestamp and the expiry of the ticket.
2. Verify the timestamp using a shared key $K_{MR1--MC}$ (Computed by mesh router 1).
3. If the verification of the time stamp is done successfully, then mesh client is considered as an authentic user or trustable user.
4. Latter on Mesh client and mesh router 1 generate a session key $H1(K_{MC--MR1})\{t1||t2\}$.

3.2 Intra-Domain Authentication

When mesh client roams from mesh router 1 to mesh router 2, Intra-domain authentication has been taking place between the mesh router and the mesh client. Following an authentication process will be followed by MC and MR_2.

1. $MR_2 \rightarrow MC: = TK_{R2}^{B1MG1}\{\mathrm{Exp}.ID_{B1}, t_{B1}, ID_{MG1}, ID_{MR2}, \mathrm{Sig}(\text{gateway})\}.$

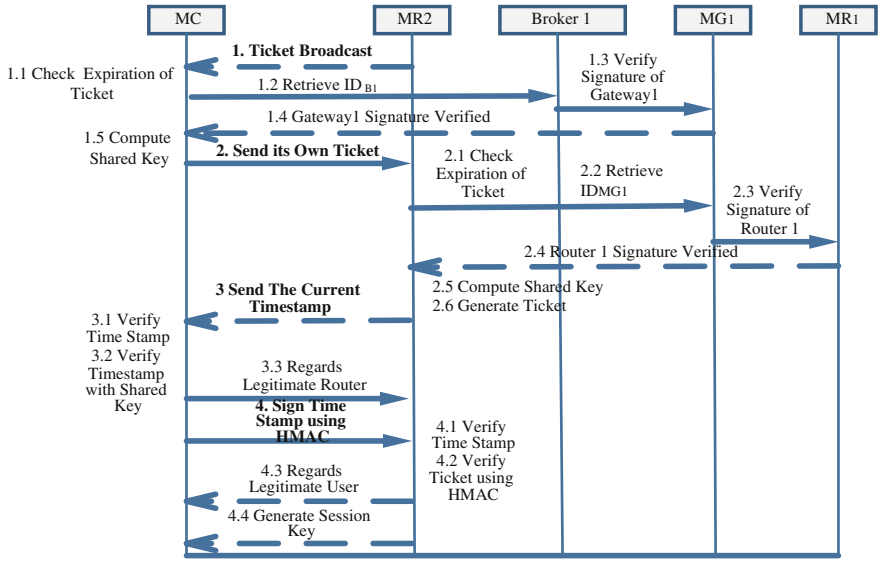

Fig. 3 Intra-Domain authentication

2. $MC \rightarrow MR_2: = TK_{MC}^{MG1MR1}\{\text{Exp}', ID_{MG1}, ID_{MR1}, ID_{MC}, \text{Sig (mesh router 1)}\}$.

3. $MR_2 \rightarrow MC: = \{t_3, N_3\}$.

4. $MC \rightarrow MR_2: = \{t_4, N_4\}$.

Mesh router 2 periodically broadcast message 1 to its coverage area. When mesh client roams from mesh router 1 to mesh router 2 called intra-domain. After receiving message 1 following operations are performed (Fig. 3).

1. It first checks the freshness of the Expiration or validity of the ticket.
2. Retrieve broker 1 public key and from broker's public key, it verifies the signature of gateway 1.
3. After verification, it computes the shared key $K_{MC--MR2}\Im\leftarrow e\leftarrow ID_{MC}$, $ID_{MR2}\leftarrow$, where

$$ID_{MR2} = \text{H1}(\text{Exp}, ID_{MG1}, ID_{MR2}).$$

Mesh client now sends a message (2) to mesh router 2. After receiving the message (2) it performs following tasks.

1. Check for the expiry date on the Client ticket and make certain that it is not expired.

2. Retrieve mesh gateway 1 public key and from mesh gateway public key, it verifies the signature of mesh router 1.
3. After verification, it computes the shared key $K_{MR2--MC} = \mathrm{e}\ (ID_{MR2}, ID_{MC})$.
4. Mesh router 2 generates timestamp t_3 and Before sending to the mesh client, mesh router 2 signs the timestamp with HMAC $N_3 = \{t_3\}$ HMACSig_$K_{MR2--MC}$.

Mesh router 2 now sends a message (3) to mesh client. After receiving the message (3) it performs following operations.

1. Check the newness of timestamp and the expiry of the ticket.
2. Verify the timestamp using a shared key $K_{MC--MR2}$ (Computed by mesh client).
3. If the verification of the timestamp is done successfully, then mesh router is considered as an authentic router or trustable router.
4. Generate a timestamp and create a signature on it, by signing it with the shared key $(K_{MC--MR2})$.

Mesh client now sends a message (4) to mesh router 2, after receiving a message (4) it perform the following operations.

1. Check the newness of timestamp and the expiry of the ticket.
2. Verify the timestamp using a shared key $K_{MR2--MC}$ (Computed by mesh router 1).
3. If the verification of the timestamp is done successfully, then mesh client is considered as an authentic user or trustable user.
4. Latter on Mesh client and mesh router 2 generate a session key $H1(K_{MC--MR2})\{t3||t4\}$.

3.3 Inter-Operator Authentication

When mesh client roams from mesh router 1 in One domain to mesh router 3 in other domain, Inter-Operator authentication has been taking place between the mesh router 3 and the mesh client. Following an authentication process will be followed by MC and MR_3.

1. $MR_3 \rightarrow MC: = TK_{R3}^{B1MG2}\{\mathrm{Exp}.ID_{B1}, t_{B1}, ID_{MG1}, ID_{MR3}, ID_{MG2}, \mathrm{Sig(gateway\ 2)}\}.$

2. $MC \rightarrow MR_3: = TK_{MC}^{MG1MR1}\{\mathrm{Exp}^{!}, ID_{MG1}, ID_{MR1}, ID_{MC},\ \mathrm{Sig(mesh\ router\ 1)}\}.$

3. $MR_3 \rightarrow MC: = TK_{MC}^{MR_3MG_2} = \{\mathrm{Exp}^{!}, ID_{MG2}, ID_{MR3}, ID_{MC}, \mathrm{Sig(Mesh\ router3)}t_5, N_5\}.$

4. $MC \rightarrow MR_3: = \{t_6, N_6\}.$

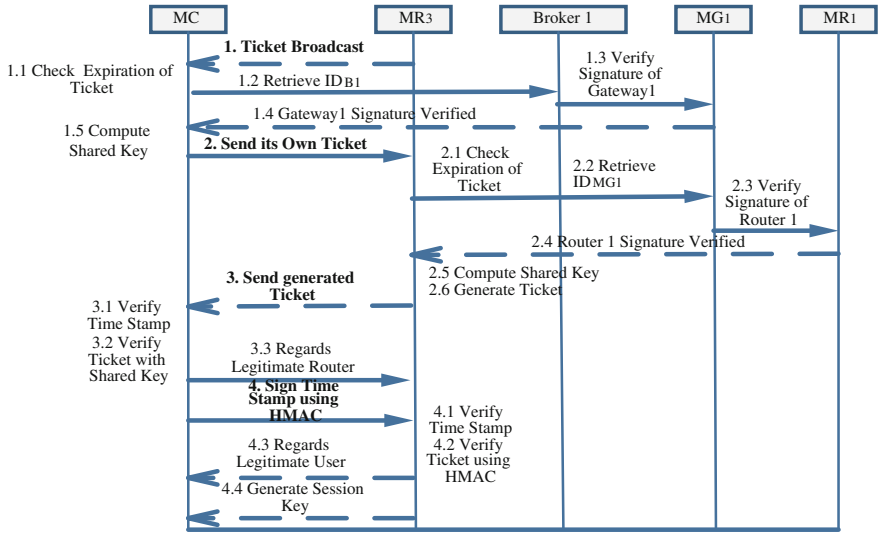

Fig. 4 Inter-Operator domain

Mesh router 3 periodically broadcast message 1 to its coverage area. When mesh client roams from mesh router 1 to mesh router 3 called an inter-Operator domain. After receiving message 1 following operations are performed (Fig. 4).

1. It first checks the freshness of the Expiration or validity of the ticket.
2. Retrieve broker 1 public key and from broker's public key, it verifies the signature of gateway 1.
3. After verification, it computes the shared key $K_{MC--MR2} = \mathrm{e}\ (ID_{MC}, ID_{MR2})$, where
4. $ID_{MR3} = \mathrm{H1}(\mathrm{Exp}, ID_{MG1}, ID_{MR3})$.

Mesh client now sends a message (2) to mesh router 3. After receiving the message (2) it performs the following tasks:

1. Check for the expiry date on the Client ticket and make certain that it is not expired.
2. Retrieve mesh gateway 1 public key and from mesh gateway public key, it verifies the signature of mesh router 1.
3. After verification, it computes the shared key $K_{MR3--MC} = \mathrm{e}\ (ID_{MR3}, ID_{MC})$.
4. Mesh router 3 generates time stamp t_5 and before sending to the mesh client, mesh router 3 signs the time stamp with HMAC $N_5 = \{t_5\}\mathrm{HMACSig}\_K_{MR3--MC}$.

Mesh router 3 now sends a message (3) to mesh client. After receiving the message (3) it performs the following operations:

1. Check the newness of time stamp and the expiry of the ticket.
2. Verify the time stamp using a shared key $K_{MC--MR3}$ (Computed by mesh client).
3. If the verification of the time stamp is done successfully, then mesh router is considered as an authentic router or trustable router.
4. Generate a time stamp and create a signature on it by signing it with the shared key $(K_{MC--MR3})$.

Mesh client now sends a message (4) to mesh router 3, after receiving a message (4) it performs the following operations:

1. Check the newness of time stamp and the expiry of the ticket.
2. Verify the time stamp using a shared key $K_{MR3--MC}$ (Computed by mesh router 1).
3. If the verification of the time stamp is done successfully, then mesh client is considered as an authentic user or trustable user.
4. Latter on Mesh client and mesh router 3 generate a session key $H1(K_{MC--MR3})\{t5||t6\}$.

4 Results

In this section we discourses the simulation of the projected algorithm. It also describes the framework for simulation for the proposed scheme.

System Configuration

For the simulation, we required the following system configuration:

- One GB RAM
- Core to duo Processor
- Windows or Linux Operating System
- Net bean Framework
- Mysql Database
- Net bean 7.4

This section gives the detail discussion about the results. In which we have focused on some parameters like Encryption Cost, Authentication Cost, Throughput, Key Generation, Key validation and System Delay. Now in this section I would like to discuss the various computation results in the form of graphs.

Encryption is the technique in which, any message is converted into an unreadable format, i.e. Ciphertext. This will be very helpful if any entity wishes to send some confidential information to any other party, i.e. before sending data it has to encrypt the message so that only the intended user can able to read the message. A lot of research work is going on this field. Figure 5 shows that the different encryption cost of different file size.

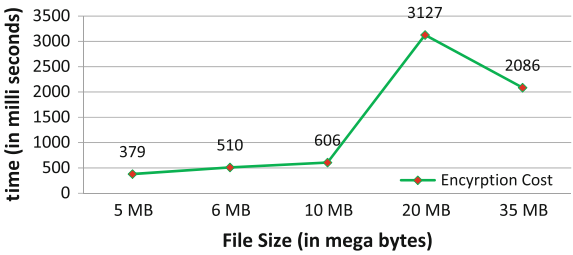

Fig. 5 Encryption cost

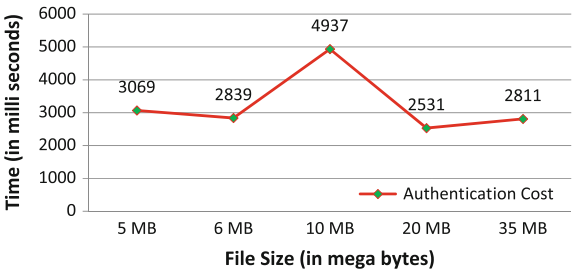

Fig. 6 Authentication cost

Authentication is an action that ensure other party that they were communicating to the legitimate user, this can be accomplished by adopting different authentication techniques. Authentication cost as its name indicates it is the cost or time required to authenticate a particular user in the network. In our case any client can able to move from one network to another. If this happens then server perform above discussed technique to authenticate the user.

A lot of research work is going on this field. Figure 6 shows that the different Authentication cost of different file size.

Network delay is one of the important parameters of performance of any type of network. We can define the network delay as the time needed to send bits of data to be traveled in the network from egress to ingress node. Delay is dependent on the location of nodes from the source to the destination node. A lot of research work is going on this field. Figure 7 shows that the different encryption costs of different file sizes.

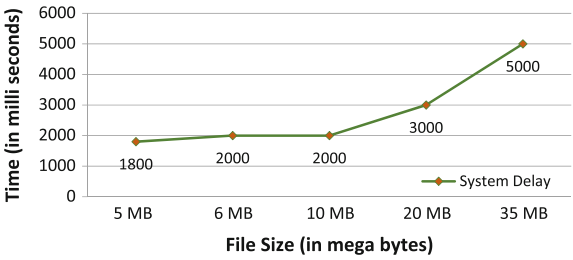

Fig. 7 System delay

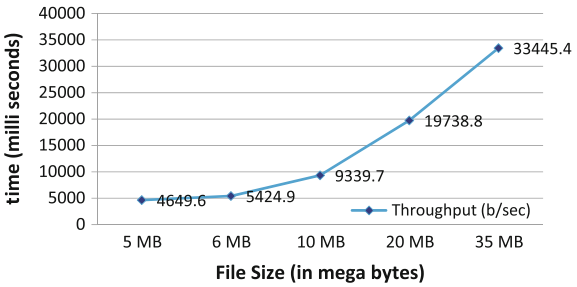

Fig. 8 Throughput

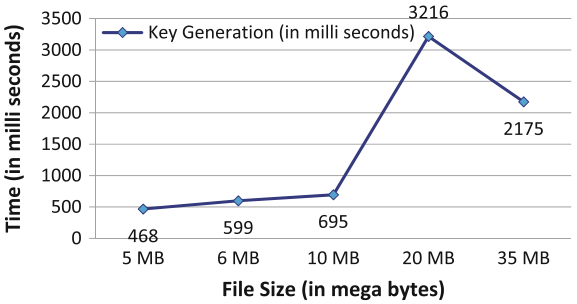

Fig. 9 Key generation

Throughput is referred as a number of bits or units of data is transferred or system is able to process in a given unit of time span. It can also be defined as a rate of successful transfer of information with the help of some channel. A lot of research work is going on this field. Figure 8 shows that the different throughput of different file sizes.

Key generation as its name indicates that any user is generating keys for further processing in the network. As we all know to communicate on the network, the public private key pair is more important. So in this key generation, we are more focused to calculate the time required to generate this public private key pair. A lot of research work is.

Going on this field. Figure 9 shows that the different Key Generation time needed for different file sizes, because here for each datum or file we compute different public private key pairs.

Key Validation as its name indicates that the truth or correctness of the keys. If any nodes from one domain to some other domain, then we perform some operation to identify that this user is a legitimate user from where it belongs. A lot of research work is going on this field. Figure 10 shows that the different key validation of different file sizes. This field is captured when a node is moving to some other network than if he wishes to send some data then how much time required is needed for key validation.

Figure 11 shows the comparison between asymmetric cryptographic techniques [11], i.e. RSA with the proposed technique. This is clearly shown that the SAWMN

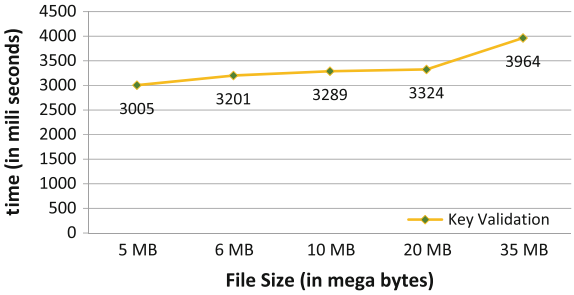

Fig. 10 Key validation

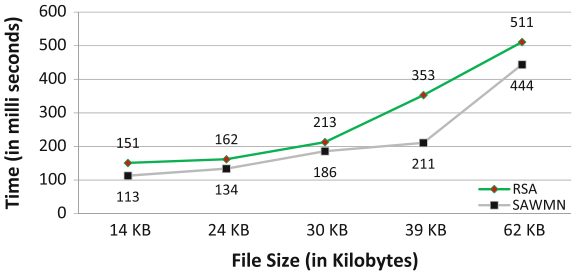

Fig. 11 Encryption technique comparisons between RSA

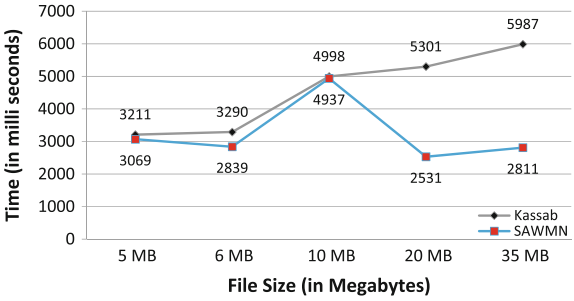

Fig. 12 Authentication cost comparison between Kassab and SAWMN

needed less time for encryption as compared to the RSA. First, we have taken the files of different sizes, then perform both the encryption on that file and record the time needed for encryption in milliseconds. Results show that our technique is much faster than the RSA.

Figure 12 shows the comparison between Authentication Cost techniques, i.e. Kassab with the proposed technique. This is clearly shown that the SAWMN needed less time for authentication as compared to the Kassab. First, we have taken the files of different sizes, then perform both the authentication on that file and record the time needed for authentication in milliseconds. Results show that our technique is much faster than the Kassab.

5 Conclusion

In this paper, we have extended the previously proposed technique in [6]. The goal of our proposed technique is to reduce the overall system complexity and overhead of the public key management. In this paper we have shown the secure authentication in the Multi-operator domain. The proposed architecture inherits the feature of delegation signing rights from Trusted Broker to other trusted node in the network. The authentication scheme is based on ticket, so it is best suited for various types of roaming, i.e. Inter-Domain. Intra-Domain and Inter-Operator domain. Furthermore, we have incorporated the identity-based encryption technique for secure information exchange among nodes (Mesh Client, Mesh Router and Mesh Gateway) in WMN. We also incorporated the privacy by utilizing fast HMAC into the account. Further, we have shown the simulated result which shows how authentication is performed while roaming to some other network. Our comparison result is also shown that, the overall authentication cost, system delay throughput and encryption cost is improved as compared to one of the previous proposed techniques. The result shows that this technique enhanced the authentication cost, the encryption cost of the network. Authentication protocols generally used for the assurance of the identity of the user to whom I am communicating. We have also considered the other parameters like securely generation, so that an attacker not able to do any type of attack in the network, apart from that we have also considered to reduce the overall delay in the network.

References

1. I.F Akyildiz, Xudong Wang and Weilin Wang, "*A Survey on Wireless Mesh Networks.*", IEEE Radio Communications, Volume 47(4), (2005).
2. Ben Salem, N. Hubaux, "*Securing Wireless Mesh Networks*", IEEE Wireless Communications, 13(2), pp 50–55 (2006).
3. L. Santhanam, B. Xie, D.P Agrawal, "*Secure and Efficient Authentication in Wireless Mesh Networks using Merkle Trees*", 33rd IEEE Conference on Local Computer Networks, LCN (2008).
4. Y. Fu, J. He, R. Wang, R. Li, "*Mutual Authentication in Wireless Mesh Networks*." In: Proceedings of ICC (2008).
5. Y. Zhang, Y. Fang, "*ARSA: an Attack-Resilient Security Architecture for Multi-hop Wireless Mesh Networks*", IEEE Journal on Selected Areas in Communications, 24(10), (2006).
6. Ninni Singh and Hemraj Saini, "*Formal Verification on Secure Authentication in Wireless Mesh Network*", Second International Conference on Computer and Communication Technologies, in Springer AISC series, (2015).
7. Ford Long Wong, Hoon Wei Lim, "*Identity-based and inter-domain password authenticated key exchange for lightweight clients*", in: AINAW'07: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops, IEEE Computer Society, Washington, DC, USA, 2007, pp 544–550.
8. Her-Tyan Yeh, Hung-Min Sun, Password authenticated key exchange protocols among diverse network domains, Computers & Electrical Engineering, 31(3) (2005) 175–189.

9. Ren-Junn Hwang, Feng-Fu Su, "*A new efficient authentication protocol for mobile networks*", Computer Standards & Interfaces 28 (2) (2005) 241–252.
10. Summit R. Tuladhar, Carlos E. Caicedo, James B.D. Joshi, "*Inter-domain authentication for seamless roaming in heterogeneous wireless networks*", in: SUTC'08: Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, SUTC 2008, IEEE Computer Society, Washington, DC, USA, 2008, pp. 249–255.
11. Catherine Meadows, "*Formal methods for cryptographic protocol analysis: Emerging issues and trends*", IEEE Journal on Selected Areas in Communications 21 (2) (2003) 44–45.