Proxy Signcryption Algorithm for Interdomain Authentication in Wireless Mesh Networks

Shamimul Qamar (sqamar@kku.edu.sa)
King Khalid University

Research Article

Keywords: TTP, WMN, Authentication, security, signature

Posted Date: August 11th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1951772/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Proxy Signcryption Algorithm for Interdomain Authentication in Wireless Mesh Networks

*Shamimul Qamar 1, Sanjay Singla 2, Parveen Kumar Sharma 3 and Ajay Roy 4, Harun Bangali 5

1 Computer Science & Engineering, College of Sciences & Arts and Dhahran Al Janub, King Khalid University, Abha, Saudi Arabia; sqamar@kku.edu.sa
2 Department of Computer Science & Engineering GGSCMT, Punjab, India; dr.ssinglacs@gmail.com
3 Department of Computer Science & Engineering, CGC.Landran Mohali Punjab, India; sharmaparveen19@gmail.com
4 Faculty of Computer and Engineering, Lovely Professional University, Punjab, India; ajayroy@live.in
5 Department of Computer Engineering, King Khalid University, Abha, Saudi Arabia; hbangali@kku.edu.sa

*Corresponding Author

Abstract:
Authentication delay is main requirement for handoff in wireless mesh networks. When mobile client moves from one domain to another. In order to solve the problems, we propose an algorithm for handoff in Wireless Mesh Networks. pre-authentication are done by mobile station itself up to the next access point. Neighbor graph is used for maintaining and dynamically identifying the mobile topology of the network. Proxy signcryption scheme is applied between the Mesh Node (MN) and mobile client (MC) for the period of inter-domain authentication. To make sure security, the authentication messages are encrypted while transmitted between mobile client and mesh nodes and signed in an integrated fashion such that the communicated message is expressed as signcrypted. Simulation’s output shows, that the algorithm strengthen security of network.

Keywords: TTP, WMN, Authentication, security, signature
1.0 Introduction

Wireless mesh network is a next generation advance technology for the Internet services, due to its ability to handle the densely growing communication network [1]. The Wireless Mesh Network is an collection of access points mesh routers, mesh clients. The mesh clients can either be static or dynamic in nature. Desktops, database servers, etc are examples of static mesh clients. Cell phones, laptops, PDA, etc are examples of mobile mesh clients in the WMN. Mesh point (MP) accelerate multi-hop connection between mesh clients or and internet by creating a wireless mesh infrastructure. A mesh access point (MAP) is formed by a collection of mesh points, and it helps in linking the mesh client with the WMN. When a mesh point is responsible for linking the WMN with the Internet, then it is referred as a gateway. Basically, WMN is a self-configuring network since the nodes inWMN connect themselves with the network and then maintain the connections as per the network requirements. Due to these characteristics of the WMN, several advantages have been seen in IEEE 802.11 based mesh network [2]. As a result of its beneficial features, WMN effective used for large space of applications like community, metropolitan area network, enterprise, etc. WMN is considered as the best backhaul technique [3]. Due to vibrant state of WMN handoff delay is one of the present-day issue of research. In common, handoff is explained as the motion of a client from one router’s radius to another routers radius. Due to mobile nature, client may far away from the mesh router, so there is requirement for client to search new mesh router to get the quick network facility.

1.2 Motivation and Proposed Solution

One of the critical challenges in WMN is handling of mobility since it is a basic requirement for wireless communication. Handoff is a process of change of client’s attachment point as it moves along the network. When an MP moves far from the current network, it will lose its connection. Hence it is necessary to handover to some other appropriate MP so as to maintain the network access [17]. To keep secure and fast-roaming capacity of the MP through various trust domains, it is significant to grant mutual authentication and key agreement in the network [4]. To safeguard WMN from spiteful nodes and to propose excellence quality of service (QoS) to clients, it is critical to remain two mode authentication between the access node and the mesh client. This
becomes the base for the security of the overall WMN. But, the authentication signal contains the privacy details of the users. Hence safeguarding the user’s isolation details is necessary during the mutual authentication method. Several types of research are carried out in the field of WMN access security to provide secure as well as proficient access authentication in WMN [5] [15]. The research in the WMN is performed on the basis of shared key mechanism. This mechanism is largely reliant on key management [11]. The public key infrastructure (PKI) require large storage requirement for storing the public key certificates [12]. Handoff latency is a time consumed by the mobile node, when it moves from its range to another routers range to authenticate itself. Pre-authentication scheme is proposed to minimize handoff latency.

This manuscript extends the earlier work [13][14] by developing pre-authentication and proxy signcryption algorithm for fast handoff in WMN.

2. Related Works

Zhang X et al [4] presented a new ID-based signcryption scheme. In this system, during the authentication stage, the mutual authentication as well as key establishment is attained between any two involved mesh points which reside in separate domain in just a pair of message exchange. The authentication message contains the data which is being communicated between two mesh points. The proposed technique can be applied to real time WMN, since there is no limitation on the PKG system factors. Random oracle model is used to demonstrate the security features of the signcryption mechanism and shows that the proposed protocol fulfills the fundamental security needs and is capable of overcoming the conventional attacks.

Daly.I et al [6] presented re-authentication mechanism to secure mobile client handoff. While taken into account of mobility factor, notification Message process is in use to execute handoff in the network. Based on the experimental study, it is seen that this mechanism can offer a secure network as well as it is a very promising re-authentication mechanism when considered with respect to compact handoff latency, minimized blocking and loss rates, etc.

Lai Y.M. et al [7] presented an effective handover authentication scheme which provides greater security with good scalability along with privacy maintenance. There are three main factors in the proposed scheme. This technique does not require client digital signature calculation and hence
minimizes the handover latency as well as computation cost. This factor makes the technique appropriate for mobile applications which have restricted computation power. The proposed technique can also be employed even when the MAP is not provided with good TPD and is also capable of avoiding the domino effect in the network. Also, this technique maintains privacy and ensures minimum authentication overhead.

Sen.J [8] presented a security and privacy protocol which provides user anonymity and maintains communication efficiency in WMN, by applying the Rivest’s ring signature mechanism. It guarantees safe authentication as well as secure encryption in both access network and also in the backbone network.

Yang.X et al [9] presented a handover authentication protocol for wireless networks. In this protocol user anonymity and un-traceability is ensured efficient manner. It shows that, protocol attains the extraordinary level of security and proficiency.

Akilarasu.G and Shalinie.M [16] presented a trust-based authentication and key establishment protocol in this an technique ant Colony Optimization (ACO) is used to maintain trust based model. Identity-based cryptography is used key establishment and authentication.

Yang.X et al [18] presented a new handoff authentication to diminish the handoff latency for WMN. Attribute-based encryption (ABE) used for pre-distribution of ticket and digital signature are used to authenticate the ticket between mobile client

Naif Amrif et al. 2018) [21] presented a The Ultra-Fast Handoff Authentication (UFAP) for token-based system which reduces the authentication delay. An authentication server are used to authentication the client to be able to use UFAP.

Then Block Chain-based approach for secure Handoff (suraj Malik et al. 2019) [22] involves high storage and computational overheads. The anonymous batch handover authentication protocol (Dongcheng et al. 2018) [23] uses group signature scheme. But since it uses elliptic curve cryptography (ECC) for group signature, it involves huge computational overhead.

Dongcheng et al. 2018 [23] uses group signature scheme. But since it uses elliptic curve cryptography (ECC) for group signature, it involves huge computational overhead.

Quang et al[24] use key for real time synchronization among tranceiever .keys are used for encryption and to avoid external attack.

Rathee et al. [26] presented a secure handoff with reduces authentication delay wireless mesh network, Authentication server are used for generating ticket for mesh router to clients, it reduce
storage overhead and security threats at client. Technique is reduce and certify over
erification delay and different situation of authentication.

[27] ticket-based handoff authentication offer a secure handoff in the environment of man in middle
attackers for multi hop system and identify the man in middle attack.

Rathee et al. [28] Fast Handoff Technique (FHT) is used. Client authenticate itself as a legitimate
node to its FMR in order to get the set-up service. technique is compared and evaluated over the
network metrics i.e. handoff latency and computational overhead.

Zhang [30] ticket based authentication protocol uses mutual authentication for multihop
environment first for pre authentication and other for fast handoff. Access point uses Pre-
distribution of keys to authenticate mobile client. Protocol is efficient in case of authentication
delay and communications costs and resilient to various attacks and also minimize the latency

3.0 Pre-Authentication and Proxy Signcryption Algorithm (PPSA)

3.1 Overview

proxy signcryption technique is applied to authenticate the movement between client and router
in the same domain or in other domain to the network. Original authority create alternate signer,
so that it can be used on its behalf. The alternate signer then create a signcrypted message by using
the substitute credential and his secret key. Alternate signer sends the signcrypted message to
the selected receiver all the way through secure network. selected receiver can retrieve the
signcrypted message and verify its validity. If any mismatch occurs later, receiver can broadcast
the signature for public verification. Algorithm-2 presents the steps involved in the proxy
signcryption process.
3.2 Proxy-based Hierarchical Network Architecture

Network architecture based proxy based hierarchical [5] is taken into considered. In WMN, trust router, Domain manager, mesh router, mesh client are used. Trusted router control the number of domains manager. Domain Manager control the number of network system. Then Gateways control the mesh router. Each domain manager hold many gateway nodes. Mobile clients (MCs) may move from one network to another network with in same domain or in another domain. Consider Figure 2. In this network, Trust Router will be at the top. Domain manager get the credential from the Trust router. DM hands over the signing authority and private keys to gateway (GW), mesh routers and clients.
3.3 Construction of Logical AP Connectivity

Logical AP connectivity maintains the network topology of AP and dynamically identifies the AP to be handoff by a MS.

Let Q_i and Q_j be the APs and let c be the MC. Q_i and Q_j are said to be connected if a client re-associates between the physical positions of Q_i and Q_j through a pre-defined path of mobility. The connectivity depends on the physical topology of APs and the physical distance between them.

The undirected graph G used for logical connectivity of AP:

\[ G = (V, E), \text{ where } V = \{Q_1, Q_2, \ldots, Q_n\} \text{ be the set of all APs} \]

\[ E = \{Q_i, Q_j\} \text{ is an frame between } Q_i \text{ and } Q_j \text{ if they are connected.} \]

Then the handoff association model H(c) for c is defined as follows:

\[ H(c) = \{(Q_1, T_1), (Q_2, T_2), \ldots, (Q_n, T_n)\} \]

Here H(c) indicates that the client c handoff to Q_2 from Q_1 at time T_2, Q_3 from Q_2 at time T_3 and so on.
This model is used in fast handoff and reduces authentication delay during intra-domain handoff. Consider Figure 3. logical connectivity and figure 4 shows the physical topology of APs. The connectivity path between the APs is shown by the dotted arrows. Here AP1 and AP3 are separated from AP2 by an obstacle. So direct connectivity between AP3 and AP2 is not possible. The logical connectivity of APs corresponding to this physical topology is shown in Figure 3 and figure 4.

Fig 3: Logical connectivity of APs

Fig 4: Physical Topology of APs
3.4 Connectivity based Pre-Authentication

A MS pre-authenticates itself to the next AP, using the AP logical connectivity. To reduce the authentication delay, this process involves a pro-active key distribution phase in which keys are pre-distributed to a pair of MS and associated AP. The connectivity based pre-authentication phase is presented in algorithm-1.

Algorithm 1.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS</td>
<td>Mobile station</td>
</tr>
<tr>
<td>AP</td>
<td>Access point</td>
</tr>
<tr>
<td>Ne(AP)</td>
<td>Neighbours of the associated AP</td>
</tr>
<tr>
<td>AP&lt;sub&gt;SL&lt;/sub&gt;</td>
<td>selected AP</td>
</tr>
<tr>
<td>Server</td>
<td>AAA server</td>
</tr>
<tr>
<td>PRF</td>
<td>Pseudo Random Function</td>
</tr>
<tr>
<td>H(MS)</td>
<td>Handoff association model for MS</td>
</tr>
<tr>
<td>AA_Mes</td>
<td>Access accept message</td>
</tr>
<tr>
<td>N_REQ</td>
<td>Alert request message</td>
</tr>
<tr>
<td>N_ACC</td>
<td>Alert accept message</td>
</tr>
<tr>
<td>N_REJ</td>
<td>Alert reject message</td>
</tr>
<tr>
<td>K&lt;sub&gt;M&lt;/sub&gt;</td>
<td>master key, shared between Server and MS</td>
</tr>
<tr>
<td>K&lt;sub&gt;PM&lt;/sub&gt;</td>
<td>pair-wise master key, shared between Server, MS, AP</td>
</tr>
</tbody>
</table>

The steps involved in this technique are as follows:

1. The pair-wise master key is derived from master key as shown below

\[ K_{PMn} = PRF(K_M, K_{PMn-1} | MS\_MAC | AP\_MAC) \]  

Where \( n \) denotes the \( n^{th} \) handoff association

Eq (1) creates a \( K_{PM} \) tree with \( H(c) \).

2. The server estimates Ne(AP)

3. Server sends a N_REQ to each \( AP_j \in Ne(AP) \)

\[ \text{Server} \xrightarrow{N\_Mes} AP_j \]
4. If AP\(_j\) decides to request K\(_{PM}\), then
5. it sends a N\(_{ACC}\) message to server

\[
\text{APSL} \xrightarrow{N_{ACC}} \text{server}
\]

Else

6. it sends N\(_{REJ}\) message to server.

7. \[
\text{APSL} \xrightarrow{N_{REJ}} \text{server}
\]

End if

8. If server receives N\(_{ACC}\) message from AP\(_{SL}\), then
9. server sends AA\(_{Mes}\) which includes K\(_{PM}\) to AP\(_{SL}\)

\[
\text{Server} \xrightarrow{AA_{Mes}} \text{MS}
\]

10. server sends authorization for MS to remain connected to the network.

11. End if

12. After pre-distribution of keys, a four way hand-shake protocol of IEEE 802.1X [19] [20] is applied to guarantee the freshness of the shared keys between the moving MS and associated AP.

### 3.5 Proxy Signcryption for inter-domain Handoff.

During inter-domain authentication, proxy signcryption method is applied between the MC and MR. In this technique, the genuine signer create a substitute credential for signing authority to the proxy signer. With the help of secret key and substitute credential, it create a signcrypted message for signing purpose. Signcrypted credential are used by proxy signer to for transmission in network. Only authentic client able to recover the message content. For any problem the proxy signature use the public verification. Algorithm-2 presents the steps involved in the proxy signcryption process.
Algorithm 2

<table>
<thead>
<tr>
<th>Notations</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>S, mes</td>
<td>Signcrypted message</td>
</tr>
<tr>
<td>C_o</td>
<td>Original signer</td>
</tr>
<tr>
<td>C_r</td>
<td>Proxy signer</td>
</tr>
<tr>
<td>C_D</td>
<td>Designated recipient</td>
</tr>
<tr>
<td>M_1 and M_2</td>
<td>Two groups of the same prime order a</td>
</tr>
<tr>
<td>V</td>
<td>Generator of M_1</td>
</tr>
<tr>
<td>S</td>
<td>System Authority</td>
</tr>
<tr>
<td>o_1</td>
<td>random number</td>
</tr>
<tr>
<td>r</td>
<td>warrant</td>
</tr>
<tr>
<td>f_0</td>
<td>random number</td>
</tr>
</tbody>
</table>

1. Initially S selects a pairing function $b: M_1 \times M_2 \rightarrow M_2$ and four collision resistant one way hash functions:

$$h_1: \{0,1\}^k \times M_1 \rightarrow \mathbb{Z}_a$$

$$h_2: \{0,1\}^k \times M_1 \rightarrow \mathbb{Z}_a$$

$$h_3: M_1 \rightarrow M_1$$

$$h_4: M_2 \times M_1 \rightarrow \{0,1\}^k$$

2. S publishes $(M_1, M_2, a, V, e, e(V, V), h_1, h_2, h_3, h_4)$ as its public parameters

3. The signer also selects a random number $f_i$ as his private key and then computes his relevant public key $U_i = f_i V$ (1)

4. If $C_o$ wish to hand over his signing authority to a proxy signer, he computes

$$O_1 = o_1 V \quad (2)$$

$$B_0 = f_0 + h_1(\tau, O_1) o_1 \mod a \quad (3)$$

5. $C_o$ then sends the proxy credential $(O_1, B_0, \tau)$ to $C_p$

6. $C_p$ then verifies its validity by computing the values at both sides of the equality symbol in the following equation:

$$B_0 V = U_0 + h_1(\tau, O_1) O_1 \quad (4)$$
7. If (4) holds with the two computed values, the proxy credential is accepted. Otherwise, the proxy credential signature is rejected.

\[ B_0V = (f_0 + h_1(\tau, O_1) O_1)V \]

\[ = f_0V + h_1(\tau, O_1) O_1V \quad (5) \]

\[ = U_0 + h_1(\tau, O_1) O_1 \]

where \( f_0V = U_0 \)

\[ O_1 = o_1V \]

8. In order to generate a signcrypted message for the message \( m \), \( C_p \) computes

\[ O_2 = o_2V \quad (7) \]

\[ B_p = \frac{1}{o_2h_2(g, \tau, O_1, O_2) + f_p + B_0} V \quad (8) \]

Secret key \( K = e(h_3(B_0 U_r), f_p U_r) \) \( (9) \)

\[ F = E_K(B_p) \quad (10) \]

\[ U = h_4(K, O_2) \oplus g \quad (11) \]

9. \( C_p \) sends the signcrypted message \((O_1, O_2, F, U)\) and \( \tau \) to \( C_r \)

10. After receiving signcrypted message \((O_1, O_2, F, U)\), \( C_r \) first recovers the message \( g \) by computing the following equations:

\[ K = e(h_3(f_p(U_0+h_1(\tau, O_1))O_1, f_p U_r) \quad (12) \]

\[ g = h_4(K, O_2) \oplus U \quad (13) \]

11. \( C_r \) computes,

\[ B_p = T_K(F) \quad (14) \]

12. \( C_r \) then verifies the validity of the proxy signature \((O_1, O_2, B_p)\) by computing the values at both sides of the equality symbol

\[ e(h_2(g, \tau, O_1, O_2) O_2 + C_r + U_0 + h_1(\tau, O_1) O_1, B_p) = e(V, V) \quad (15) \]

13. If eq (15) holds with the two computed values, then \( C_r \) accepts the proxy signature. Otherwise, he/she rejects the proxy signature.
Note: \((V, V)\) is pre-computed as one of the public parameters during system setup phase; Hence, the computational cost for this value can be ignored.

14. If there is a dispute between the proxy signer and recipient, \(U_r\) can send the message \(g, \tau\) and proxy signature \((O_1, O_2, B_p)\) to any trusted third party.

15. A trusted third party uses Eq (15) to perform an evaluation task and identifies whether \(C_p\) is dishonest.

According to our architecture shown in Figure 2, if a MC handoff from domain1 to domain2, and connect with MR4 of WMN3, then MC becomes the original signer, GW1 becomes the proxy signer and MR4 becomes the designated receiver. TR becomes the system authority.

### 4.0 Performance Evaluation

The proposed Pre-Authentication and Proxy Signcryption Algorithm (PPSA) is simulated in network simulator-2. Security and authentication is the main concern of the work, so number of node are varying and the maximum node up to 48, stretch crossways 3 base stations (BSs) within an region of 1250x1250 meter square. The 3 BSs are associated with in network. The numbers of attackers are varying from 1 to 5. The propagation model CBR and omni Antenna are considered.

Table 1 is shows setting and parameters for simulation

<table>
<thead>
<tr>
<th>Mobile Nodes</th>
<th>4,6,8,10,12 and 16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area of Size</td>
<td>1250 x 1250m</td>
</tr>
<tr>
<td>Medium Access</td>
<td></td>
</tr>
<tr>
<td>Control Protocol</td>
<td>IEEE 802.11</td>
</tr>
<tr>
<td>Time for Simulation</td>
<td>50 second</td>
</tr>
</tbody>
</table>
### 4.2 Performance Metrics

The proposed PPSA is compared with protocol IPGS [6] and TBHA [3]. In this simulation, there are 16 number of nodes per base station and the number of attackers are varied from 1 to 5 the performance are measured as per metrics communication delay, authentication delay, delivery ratio, packet drop, compromised cost.

Since PPSA uses connectivity based pre-authentication phase, it reduces the authentication delay. The count of key used is less. It provides privacy and validation by proxy signcryption technique.

### 4.3 Results and Analysis

**A. On the Nodes Basis**

In the simulation the nodes are wide-ranging from 4, 6, 8, 10, 12 and 16.
The delay vs Nodes shown by Figure 5 for PPSA, IPGS and TBHA. The delay of PPSA extend from 2.6 to 7.9, the delay of IPGS extend from 8.3 to 10.5 and the delay of TBHA extend from 9.2 to 13.0. Hence the delay of PPSA is 50% and 57% of less when contrast to IPGS and TBHA.

**Fig 5: Nodes Vs Delay**

**Fig 6: Nodes Vs Delivery Ratio**
The Node Vs delivery ratio shown in Figure 5, when PPSA compared with IPGS and TBHA, the delivery ratio of PPSA reduce from 0.72 to 0.63, delivery ratio of IPGS reduce from 0.592 to 0.510 and the delivery ratio of TBHA reduce from 0.521 to 0.452. Hence PPSA is elevated 28% and 35% when contrast IPGS and TBHA.

![Fig 7: Nodes Vs Packet Drop](image)

The Node Vs drop shows in Figure 6 for PPSA, IPGS and TBHA. The drop of PPSA rise from 5779 to 25529, the drop of IPGS rise from 12150 to 40643 and the drop of TBHA rise from 16325 to 43185. Hence the drop of PPSA is 50% and 60% less when contrast IPGS and TBHA.

![Percentage of Compromised Nodes](image)
Figure 8 shows the Nodes Vs percentage of compromised nodes. The compromised nodes of PPSA decreases from 12.7 to 12.0, the compromised nodes of IPGS increases from 11.5 to 15.2 and the compromised nodes of TBHA increases from 14.2 to 16.6. Hence the compromised nodes of PPSA are 5% and 22% less when contrast to IPGS and TBHA.

![Communication Cost Chart](chart.png)

Figure 9: Nodes Vs Communication cost

The Nodes Vs communication cost shows in figure 8. The communication cost of PPSA increases from 12.4 to 15.4, the communication cost of IPGS increases from 13.0 to 17.0 and the communication cost of TBHA increases from 14.5 to 18.1. Hence the communication cost of PPSA is 9% and 17% of less when contrast to IPGS and TBHA.
A. On the Basis of Attackers

In simulation the number of attackers are varied as 1, 2, 3, 4 and 5.

Fig 10: Attackers Vs Delay

The Attacker Vs delay shows in figure 10. The delay of PPSA extends from 0.8 to 13.4, the delay of IPGS extends from 6.2 to 15.1 and the delay of TBHA extends from 6.2 to 15.7. Hence the delay of PPSA is 30% and 36% less when contrast to IPGS and TBHA.

Fig 11: Attackers Vs Delivery Ratio
Attackers Vs delivery ratio shows in figure 11. Delivery ratio of PPSA reduce from 0.9 to 0.3, the delivery ratio of IPGS reduce from 0.71 to 0.21 and the delivery ratio of TBHA reduce from 0.72 to 0.31. Hence the delivery ratio of PPSA is 26% and 30% elevated when contrast to IPGS and TBHA.

![Graph of PacketDrop vs Attackers](image1)

**Fig 12: Attackers Vs Packet Drop**

The Attacker Vs drop shows Figure 12. The drop of PPSA rise from 6365 to 45955, the drop of IPGS rise from 25458 to 65841 and the drop of TBHA rise from 21943 to 73980. Hence the drop of PPSA is 40% and 46% less when compared to IPGS and TBHA.

![Graph of Percentage of Compromised Nodes vs Attackers](image2)

**Fig 13: Attackers Vs Compromised Nodes**
The Attackers Vs percentage of compromised nodes shows Figure 13. The compromised nodes of PPSA decreases from 8.7 to 17.3, the compromised nodes of IPGS increases from 11.7 to 21.29 and the compromised nodes of TBHA increases from 13.6 to 26.07. Hence the compromised nodes of PPSA are 18% and 28% less when contrast to IPGS and TBHA.

![Communication Cost Graph](image)

**Fig 14**: Attackers Vs Communication

The Attackers Vs communication cost shows in Figure 14. the communication cost of PPSA increases from 10.0 to 19.1, the communication cost of IPGS increases from 14.9 to 21.2 and the communication cost of TBHA increases from 15.2 to 21.5. Hence the communication cost of PPSA is 15% and 18% less when contrast to IPGS and TBHA.

### 5.0 Conclusions

Proxy signcryption process is applied for the router and client during inter-domain authentication. In this scheme, unique signer generates a substitute credential to hand over his signing authority to the alternate signer. The alternate signer creates a signcrypted message by using the substitute credential and his secret key. Then alternate signer sends the signcrypted message to a selected receiver all the way through secure network.

By experimental results, it shows that proposed technique increase network security and quality of service with reduced packet drop, Packet delay, compromised cost, communication cost, and higher packet delivery Ratio by varying number of attacker and varying number of Nodes on comparsion of PPSA with IPGS and TBHA with secure and fast handoff. It shows that proposed scheme has efficient and quick handoff as compared to other techniques.
**Acknowledgements:**

The authors would like to express their gratitude to the Deanship of Scientific Research, King Khalid University, Abha, Saudi Arabia, to provide administrative, financial, and technical support under Grant Number GRP 155/1443.

Declarations Conflict of interest: The authors have no conflict of interest.

**References**


https://doi.org/10.3837/tiis.2015.07.10


https://doi.org/10.1371/journal.pone.0155064


