Trust Based Authentication and Key Establishment for Secure Routing in WMN

G.Akilarasu[1] and Dr.S.Mercy Shalinie[2]
[1]Research Scholar, Dept. of Computer Science and Engineering,
Thiagarajar College of Engineering, Madurai-625015, India
akilarasu0684@gmail.com
[2]Associate Professor and Head Department of Computer Science and Engineering,
Thiagarajar College of Engineering, Madurai-625015, India

Abstract

In Wireless Mesh Networks (WMN), an authentication technique can be compromised due to the distributed network architecture, the broadcast nature of the wireless medium and dynamic network topology. Several vulnerabilities exist in different protocols for WMNs. Hence, in this paper, we propose trust based authentication and key establishment for secure routing in WMN. Initially, a trust model is designed based on Ant Colony Optimization (ACO) to exchange the trust information among the nodes. The routing table is utilized to select the destination nodes, for which the link information is updated and the route verification is performed. Based on the trust model, mutual authentication is applied. When a node moves from one operator to another for accessing the router, inter-authentication will be performed. When a node moves within the operator for accessing the router, then intra-authentication will be performed. During authentication, keys are established using identity based cryptography technique. By simulation results, we show that the proposed technique enhances the packet delivery ratio and resilience with reduced drop and overhead.

Keywords: Wireless Mesh Networks, Trust, Authentication, Ant Colony Optimization (ACO) and Key establishment

http://dx.doi.org/10.3837/tiis.2014.12.024

1. Introduction

1.1 Wireless Mesh Network (WMN)

A communication network that comprises of radio nodes that are arranged in a mesh topology is defined as Wireless Mesh Network (WMN). Sometimes, WMN is defined as a superset of ad hoc networks. Client WMN has mobile client devices whereas an infrastructure WMN has mesh routers [1][2].

Nodes in WMN are of two types. They are:

(i) **Mesh routers** are the fixed nodes with one or more wireless interfaces to offer a backbone infrastructure that is managed through routing protocols.

(ii) Mesh clients: Mesh clients are either fixed or mobile terminal hosts. The routing protocols are constantly victims of attacks who are attempting to compromise their capabilities [3].

WMN is often affected due to black hole and gray hole attacks. Black hole is a compromised node that attracts the traffic using forged routing messages to drop the packets maliciously. However, gray hole drops the packets, selectively. In other words, gray hole forwards the routing packets while dropping the data. By this way, gray hole enters the path discovery phase to interrupt the data from reaching the destination. This attack may cause serious problems as it makes all the data protection mechanisms to fail [3].

1.2 Secured Routing in WMN

Each node can either operate as a host or as a router to forward the data packets, if the other nodes are not located within the direct wireless transmission range of the destinations. In order to lessen the cabling cost for building infrastructure and to support internet access to the users, multihop wireless connectivity among these routers is used.

As security in WSN is easily compromised, there are no efficient and scalable security solutions. WSN is easily attacked due to the susceptibility of channels and nodes in the shared wireless medium, dependence upon neighbors, dynamic variation in network topology and resource constraints.

Therefore, the accuracy of routing information is significant to any routing protocol. The security requirements of routing protocols are:

- **Authentication:** During this process, nodes check each routing message whether it is sent by a legitimate node or not. Secure authentication has communicating entities to check the authenticity of each other. It generates the shared common session keys. These keys are utilized in cryptographic algorithms to impose the message confidentiality and integrity.
- **Integrity:** Here, nodes validate the integrity of received routing message by checking whether the message is altered or not [4][5].

Due to the presence of distributed network architecture dynamic network topology, weak authentication schemes can be easily attacked. Vulnerabilities in routing protocols can be exploited by the potential attackers for reducing the performance of the network. Nodes need the cooperation of other nodes in the network to operate in a successful manner.

In WMN, Medium Access Control (MAC) layer and network layer protocols assume that the participating nodes are genuine with no malicious or dishonest intentions. However, some nodes behave in a selfish manner. Then, it is compromised by the malicious users. The MAC and the network layer protocols are vulnerable to various attacks because of the assumed trust and the absence of accountability. This is mainly due to the lack of central administration.

The attacks that are related to authentication in WMNs are as follows: (i) unauthorized access, (ii) replay attack, (iii) spoofing attack, (iv) Denial of Service (DoS) attack, (v) intentional collision of frames, (vi) pre-computation and partial matching attack and (vi) Compromised or forged MRs [12].

1.3 Problem Identification

As the network has several compromised nodes and attacks, providing security to the network is essential. Some of the existing works discussed about the authentication and integrity. Some other works in literature discussed about the elimination of worm hole attack. There is no combined technique to eliminate the Wormhole attack along with authentication and integrity. Hence, a Trust Based Authentication and Key Establishment for Secure Routing in WMN is proposed.

The rest of the paper proceeds as follows. Section 2 analyzes the existing works related to the proposed work. The proposed solution will be presented in section 3. Section 4 evaluates the proposed solution through simulations. Conclusions are provided in section 5.

2. Literature Review

Shams Qazi et al [4] have proposed a cross-layer secure protocol for routing, data exchange and ARP problems (in case of LAN based upon WMNs). This is a Ticket-based Adhoc On demand Distance Vector (TAODV) protocol, a secure routing protocol that is based on the design of Ad hoc On demand Distance Vector (AODV) protocol. Due to the availability of backbone, they incorporate the Authentication Server (AS) for the issuance of tickets, which are further used for secure routing, transfer of public keys and MAC addresses in one single step. With the transfer of public keys, source and destination can easily generate their shared secret key based upon Fixed Diffie-Hellman key exchange protocol for data encryption and decryption. Their protocol is secure against both active and passive attacks. However, there exists network traffic.

Tianhan GAO et al [5] have proposed a delegation based authentication scheme under broker-based hierarchical security architecture and trust model. Mutual authentication is achieved directly between mesh clients and access mesh router though ticket, which is equipped with identity-based proxy signature. Fast authentication for different roaming scenarios is supported using HMAC operations on both mesh client side and mesh router side. As a byproduct, key agreement among participants is also implemented to protect the subsequent communications. Security analysis demonstrates that their proposed scheme is resilient to various kinds of attacks. However, the mutual authentication is failed as the valid signature on messages could not be produced without entity’s secret key.

Bing He and Dharma P. Agrawal [6] have proposed an authentication and key establishment scheme for WMN base on the Identity-Based Cryptography (IBC), which enables the efficient key agreement and mutual authentication between network entities in a WMN. Through this distributed authentication key establishment scheme, the network entities can authenticate each other and establish pairwise communication keys with substantially reduced communication overhead and authentication delay. However, there occurs the delay in authentication.

Chen Dajun et al [7] have proposed an ant-based trusted routing algorithm for WMNs. The experimental results indicate that this algorithm achieves improvements in terms of end-to-end delay, packet delivery ratio and routing overhead compared with typical DSR protocol and AODV protocol. However, the routing overhead is increased.

Ramya R et al [8] have proposed a Secured Identity Based Routing (SIBR) scheme in which every node is assigned with security cards for providing an efficient authentication. The major goal of the proposed system is to reduce the number of levels at which an attack can take place by providing anonymity in routing. This scheme increases the overall performance of the network substantially. Such a routing scheme enhances the privacy preservation of the end users. This approach also protects against performance degradation even in the presence of malicious behavior.

Farah Kandah and Yashaswi Sin [9] have presented an effective Secure Key Management Scheme (SKeMS), which seeks an encryption key assignment such that the induced network is securely key connected and well protected against potential malicious eavesdropping attacks. This scheme assigns available encryption keys among all the nodes in the network. This provides a network that is resistant to malicious eavesdropping attack. However, the vulnerability is not removed completely.

Tianhan GAO et al [10] have proposed a novel privacy-preserving authentication scheme upon hierarchical security architecture in order to guard mobile users' access. Anonymity is achieved in light of a trilateral pseudonym approach without key escrow. The pseudonym is able to be alerted by mobile user at will against the link ability attack from adversaries. The key agreement mechanism is also incorporated into this scheme to protect subsequent communications between mobiles users and access network.

Xin Zhao et al [11] have proposed ECC based Self-Certified Public Key Cryptosystem (ECCSCPKC) for constructing WMNs security infrastructure, and its related security schemes with a few modifications are used for designing the AKA protocol. This scheme supports an efficient authentication and key agreement between a mesh client and a mesh router, with less cost of communication and computation resources as well as system maintenance. However, the fault tolerance has to be improved.

3. Proposed Solution

In this paper, we propose to trust based authentication and key establishment for secure routing in WMN. Initially, a trust model is designed based on Ant Colony Optimization (ACO). This model involves exchanging the trust information among the nodes. The routing table is initialized for selecting the destination nodes, for which the link information is updated and the route verification is done. Based on the trust model, mutual authentication is applied. When a node moves from one operator to another operator for accessing router, then inter-authentication is performed. When the node moves within the operator for accessing the router, then intra-authentication is performed. During authentication, the keys are established using identity based cryptography technique. In **Fig. 1,** the proposed block diagram is shown.

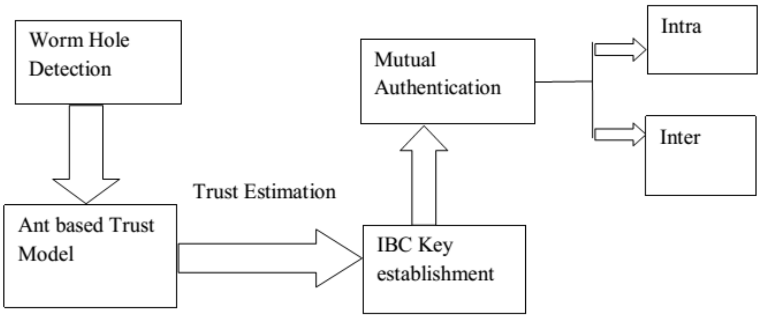

Fig. 1. Block Diagram of the Proposed Work

3.1 Estimation of Trust Value

The monitoring node initially maps its neighbors into two clusters and then classifies clusters into two types: selfish and cooperative. The clustering technique depends on single-linkage approach in which each cluster is represented by all the objects in the cluster. Also the similarity between two clusters is measured by the similarity of the closest pair of data points belonging to different cluster. This process is repeated until all the objects are merged to form cluster [13].

The clustered sets are classified into the following groups:
1. A set of cooperative nodes (C_N)
2. A set of selfish nodes (S_N).

The cooperation score (C_S) of any node in the network is computed as follows:

$$C_S = \frac{\sum_{i,j\in C_N}^{m} n_{ij}^{(r)}}{|C_N|} - \frac{\sum_{i,j\in S_N}^{m} n_{ij}^{(r)}}{|S_N|} \quad (1)$$

where,
C_S is the cooperation score
C_N is the cooperative nodes
S_N is the selfish nodes

The trust value of N_i and N_j of wireless network is estimated based on the following equation.

$$T_{ij} = (a * C_s)/(\beta * PLR_{ij}) \quad (2)$$

PLR_{ij} = packet loss rate from N_i and N_j
The constant values α and β are assigned within the range (0, 1).

3.2 Ant Based Trust Model

We consider a swarm intelligence technique based on ACO for estimating the trust value of nodes [7]. The Forward Ant agent (FA) establishes the pheromone track to the source node (S), while Backward Ant agent (BA) establishes the pheromone track to the Destination (D).

The header of the ant agents include the fields which are illustrated in **Table 1.**

Table 1. Header field of the ant agent

Node ID	Sequence number	C_S	PLR	T

The steps involved in the ant based trust model are briefly discussed below:

Algorithm-1: ***Ant based Trust establishment***

1) FA is launched in S and it traverses through all nodes along the path towards D.
2) FA on reaching every node, computes the parameters like C_S, PLR, and estimates the trust value using equation (1). It then updates its header with the information about the node (as per Table-1).
3) FA selects the next hop node N_i as per the fitness function given by

$$F(i, j) = T_{ij} \tag{3}$$

If F value of the N_i is much higher, the node N_i will be selected with the probability of 0.5, otherwise the next node Nj will be retained

4) With the collected information from all the hops, FA reaches D.
5) When FA reaches D, D generates BA and transfers all the information of FA into BA. BA takes the same path as that of its corresponding FA, but in the reverse directions.
6) BA updates the header field at the neighboring nodes for all the entries related to the FAs destination node, as per following update rules.

$$\lambda = \left\{ \frac{T_{xD}}{a\ \rho}, a \geq 1, if\ \frac{T_{xD}}{a\rho} < 1 \right. \tag{4}$$

Where a = 2

T_{xD} = trust from N_x to D

ρ = average trust value

7) The trust value of the node is updated using following equation.

$$\rho_D = \rho_D + \sigma'(T_{xD} - \rho_D) \tag{5}$$

$$\alpha_D^2 = \alpha_D^2 + \sigma'((T_{xD} - \rho_D)^2 - \alpha_D^2 \tag{6}$$

where ρ_D = average trust value from local node to D

α_D^2 = trust variance

8) BA upon reaching S delivers the status of all the nodes. Each node obtains the routing table to be used to select the next node using probability value.
9) The source then selects the nodes with the maximum trust value.

3.3 Key Establishment

3.3.1. Establishment of pairwise key

This section describes about the establishment of pairwise key between the two nodes X and Y. This can be explained in the following steps:

Step 1: In order to establish a pairwise key, the node establishes a pairwise master key (K_{mp}).

Step 2: Sending of Response Message

Once the pairwise session key is established, a pairwise session key (K_{PS}) is used to protect the unicast threat between two participant nodes. For instance: by considering challenge-response style protocol, node X sends a challenge in the form $(X \rightarrow Y)$

$$X, XXX_X, Q_{K_{mp}}(X,Y)(nonce_X), Framenumber\ Y, XXX_Y \tag{7}$$

Where X, and XXX_X represent ID of node X and its home domain, respectively.
Y, and XXX_Y represents ID of the node Y and its home domain XXX, respectively.
nonce X represents the random number created by X and it is encrypted with the help of pairwise master key K_{mp} (X, Y), which is denoted as $Q_{K_{mp}}(X,Y)(nonce_X)$.

Frame number represents auto increase message, which is used as a time stamp which assures that message is free from attack. Hence both the participating node checks for the timestamp each and every time once they receive the message.
Step 3: The response message is then sent from node $X \rightarrow Y$ as below:

$$Y, XXX_Y, Q_{K_{mp}}(X,Y)(nonce_Y), Framenumber\ X, XXX_X \tag{8}$$

Where $nonce_Y$ represents random number created by node Y
$Q_{K_{mp}}(X,Y)(nonce_Y)$ represents encrypted nonce Y by the K_{mp} (X, Y).
Step 4: Decryption of received message
Node X and Y decrypts the received message by K_{mp} (X, Y) and hence both get $nonce_X$ and $nonce_Y$.
Step 5: The pairwise session key K_{PS} is calculated as follows:

$$K_{PS}(X,Y) = U(X, Y, nonce_X, nonce_Y) \tag{9}$$

Where U () represents keying hash function

3.4 Mutual Authentication

3.4.1 Format of Ticket

There are two types of ticket considered for authentication: Direct and Delegation.
Direct ticket is directly issued from Distributor. The format of the ticket is given in **Table 2.**

Table 2. Format of Direct Ticket (T_R^D)

Exp	PK_D	PK_R	T_R	$SIGN_D$

Exp: Expiration time of the ticket – which is assigned based on the trust value. (ie) Nodes with lesser trust values are assigned shorter expiration time and vice versa.
The notations given in Table-2 are defined below:
PK_D : Public key of distributor
PK_R : Public key of receiver
T_R : Updated trust value of the receiver
$SIGN_D$: Signature of distributor over the ticket.

Delegating ticket is issued by Distributor, who has delegation rights from the Delegator, to the owner. The format of the ticket is given in **Table 3.**

Table 3. Format of Delegation Ticket (T_R^{DLD})

Exp	PK_{DL}	PK_D	PK_R	T_R	$SIGN_D$

Exp: Expiration time of the ticket – which is assigned based on the trust value. (ie) Nodes with lesser trust values are assigned shorter expiration time and vice versa.

The notations given in **Table 3** are defined below:

PK_{DL} : Public key of delegator
PK_D : Public key of distributor
PK_R : Public key of receiver
T_R : Updated trust value of the receiver R
$SIGN_D$: Signature of distributor over the ticket.

3.4.2 Inter-Operator Authentication

Let TA_i, GW_i, R_i, C_i be the trust authenticator, gateway, router, and client, respectively.
Let PK be the public key (established using section 3.4)
Let ϕ be the verification signature
Let TK be the ticket for identity management

When a node moves from one operator to another operator for accessing the router, then inter-authentication is performed.

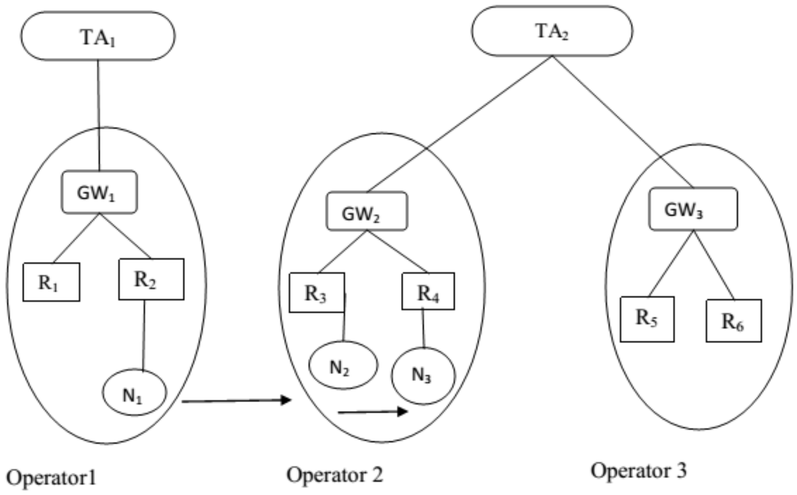

Fig. 2. Mutual Authentication

Consider **Fig. 2** N_1 moves from operator 1 to operator 2 and access router R_3. The authentication is performed as follows:

Step 1: R_3 periodically sends a beacon message to its transmission range. This message includes the ticket of R_3. This helps N_1 for detecting R_3 and joining with it.

$$TK_{R_3}^{TA_2GW_2} = SIGN_{K_{PS}}(GW_2, R_3)\{Exp, PK^{TA_2}, PK^{GW_2}, PK^{R_3}, T_R) \tag{10}$$

$$R_3 \rightarrow N_1 : TK_{R_3}^{TA_2GW_2} \tag{11}$$

Step 2: On receiving the beacon message, N_1 transmits the following message to R3 along with N_i's ticket.

$$TK_{N_1}^{TA_1} = SIGN_{K_{PS}}(TA_1, N_1)\{Exp, PK^{TA_1}, PK^{N_1}, T_R) \tag{12}$$

$$N_1 \to R_3 : TK_{N_1}^{TA_1} \tag{13}$$

Step 3: N_1 verifies whether Exp in R_3's ticket is not expired or not and recovers the valid PK^{TA2}. Then it verifies SIGN K_{PS} with valid PK^{TA2} and retrieves valid PK^{R3}.
Step 4: Upon receiving message from N_1, R_3 verifies whether Exp in N_1's ticket is expired or not and retrieves the valid PK^{TA1}. Then it verifies C_{GW1} with PK^{TA1} and retrieves valid PK^{N1}.
Step 5: R_3 then transmits the following message to N_1.

$$TK_{N_1}^{GW_2R_3} = SIGN_{K_{PS}}(GW_2, N_1)\{Exp', PK^{R_3}, PK^{GW_2}, PK^{N_1}, T_R\} \tag{14}$$

$$R_3 \to N_1 : [TK_{N_1}^{GW_2R_3} t_1, \phi_1] \tag{15}$$

Step 6: Upon receiving message from R_3, N_1 verifies whether t_1, Exp and ϕ_1 is valid. If validation is successful, N_1 will sign the timestamp and transmit the following message.

$$N_1 \to R_3 : [t_2, \phi_2] \tag{16}$$

Step 7: R_3 verifies the validity of t_2 and ϕ_2. If the validation is successful, then R_3 will accept N_1 as valid node. Thus, inter-authentication is completed.

3.4.3 Intra-Operator Authentication

When N_2 moves with in the operator for accessing the router, then the intra-authentication is performed.
Consider **Fig. 2.** N_2 moves from R_3 to R_4 within the same operator.
Step 1: R_4 transmits the beacon message to N_2

$$TK_{R_4}^{T_2GW_2} = SIGN_{KPS}(GW_2, R_4)\{Exp, PK^{TA_1}, PK^{GW_2}, PK^{R_4}, T_R\} \tag{17}$$

$$R_4 \to N_2 : TK_{R_4}^{T_2GW_2} \tag{18}$$

Step 2: N_2 transmits the following message to R_4 that includes the ticket issued by R_3

$$TK_{N_1}^{GW_2R_3} = SIGN_{K_{PS}}(R_3, N_2)\{Exp', PK^{R_3}, PK^{N_2}, T_R) \tag{19}$$

$$N_2 \to R_4 : TK_{N_1}^{GW_2R_3} \tag{20}$$

Step 3: N_1 after verifying the validity of Exp and validates SIGN K_{PS} (GW_2, R_4) with PK^{TA2} and retrieves PK^{R4}.
Step 4: R_4 upon receiving the message verifies the validity of Exp and validates SIGN K_{PS} with PK^{TA2} and retrieves PK^{N2}.
Step 5: R_4 signs the current timestamp t_3 and transmits the message as follows

$$R_4 \to N_2 : [t_3, \phi_3] \tag{21}$$

Step 6: N_2 after receiving the message verifies whether t_3 is valid and validates ϕ_3 with K_{N2-R4}. If the validation is successful, then N_2 accepts R_4 as valid router.
Step 7: N_2 signs the timestamp and resends the message as follows

$$N_2 \rightarrow R_4 : [t_4, \phi_4] \tag{22}$$

Step 7: R_4 upon receiving the message verifies the validity of t_4. Then, validates ϕ_4 with K $_{R4-N2}$ and if validation is successful, R_4 accepts N_2 has valid node. Thus, intra-authentication is completed successfully.

The flowchart for the inter- and intra-authentication is illustrated in Fig. 3 and 4, respectively.

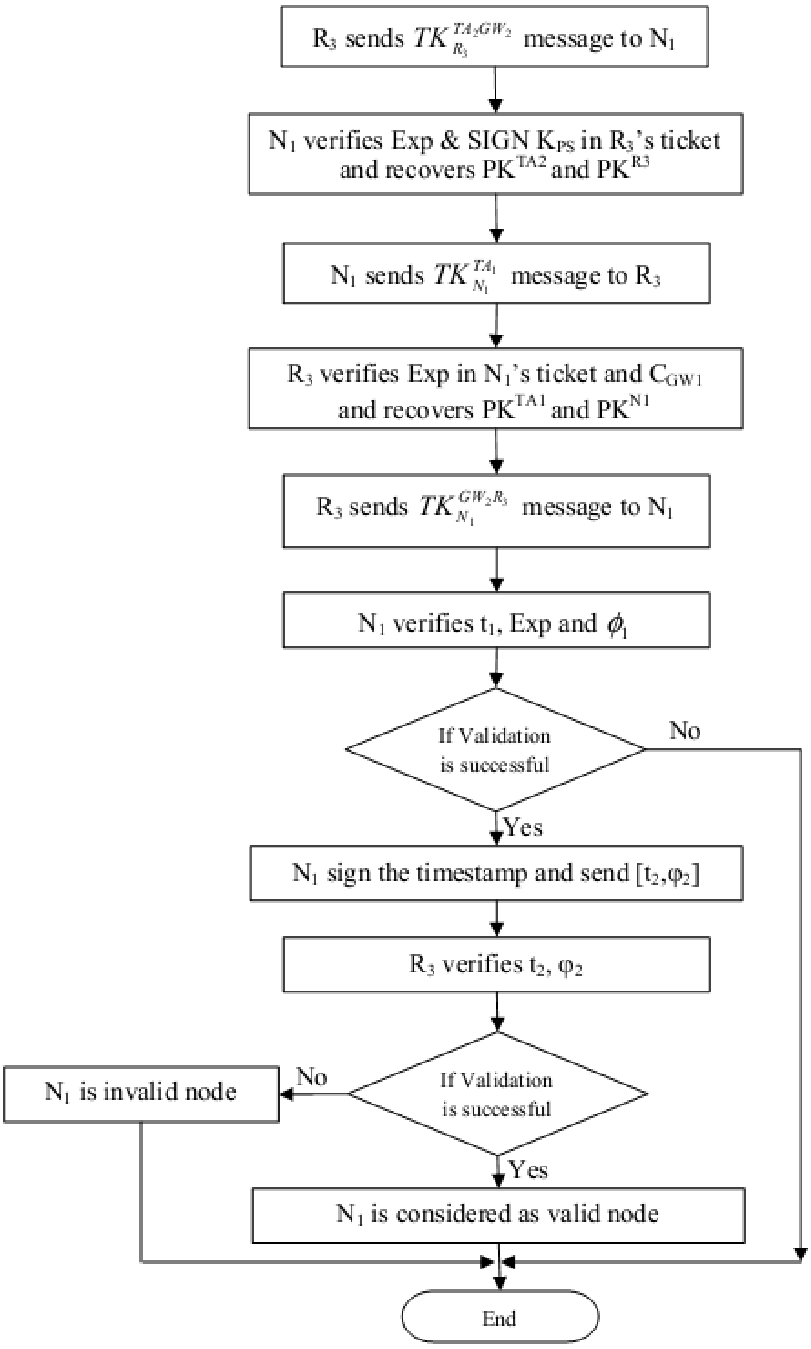
R₃ sends $TK_{R_3}^{TA_2GW_2}$ message to N₁
N₁ verifies Exp & SIGN K_PS in R₃'s ticket and recovers PK^TA2 and PK^R3
N₁ sends $TK_{N_1}^{TA_1}$ message to R₃
R₃ verifies Exp in N₁'s ticket and C_GW1 and recovers PK^TA1 and PK^N1
R₃ sends $TK_{N_1}^{GW_2R_3}$ message to N₁
N₁ verifies t₁, Exp and ϕ_1
If Validation is successful
No
Yes
N₁ sign the timestamp and send [t₂,φ₂]
R₃ verifies t₂, φ₂
If Validation is successful
No
N₁ is invalid node
Yes
N₁ is considered as valid node
End

Fig. 3. Flowchart for inter-authentication

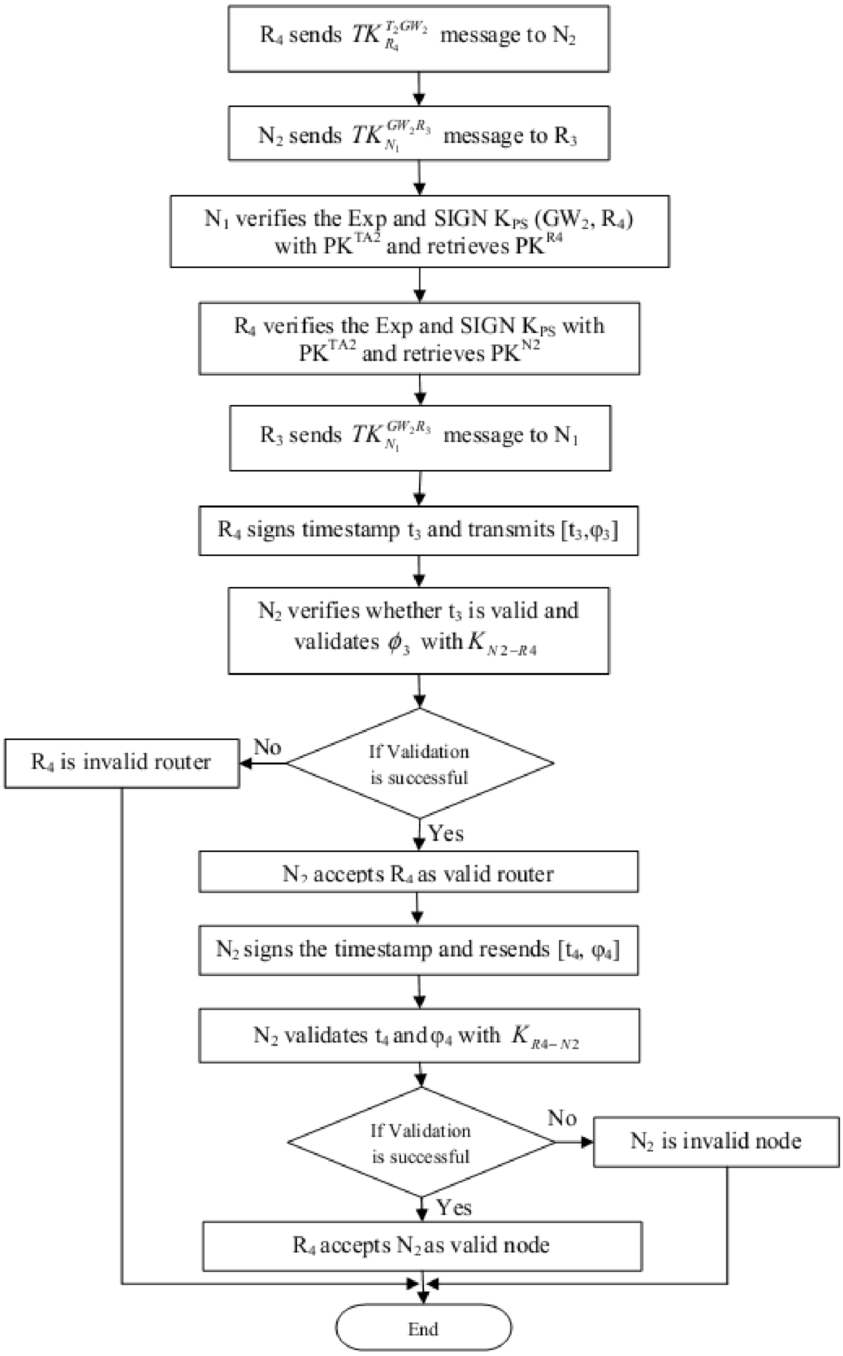
R_4 sends $TK_{R_4}^{T_2GW_2}$ message to N_2
N_2 sends $TK_{N_1}^{GW_2R_3}$ message to R_3
N_1 verifies the Exp and SIGN K_{PS} (GW_2, R_4) with PK^{TA2} and retrieves PK^{R4}
R_4 verifies the Exp and SIGN K_{PS} with PK^{TA2} and retrieves PK^{N2}
R_3 sends $TK_{N_1}^{GW_2R_3}$ message to N_1
R_4 signs timestamp t_3 and transmits [t_3,φ_3]
N_2 verifies whether t_3 is valid and validates ϕ_3 with K_{N2-R4}
If Validation is successful
No
R_4 is invalid router
Yes
N_2 accepts R_4 as valid router
N_2 signs the timestamp and resends [t_4, φ_4]
N_2 validates t_4 and φ_4 with K_{R4-N2}
If Validation is successful
No
N_2 is invalid node
Yes
R_4 accepts N_2 as valid node
End

Fig. 4. Flowchart for inter-authentication

4. Simulation Results

4.1 Simulation Model and Parameters

The Network Simulator (NS2) [13], is used to simulate the proposed work. By considering the complexity of deploying a larger mesh network, in the simulation, the scenario is restricted to 50 mobile nodes deployed in a 500 meter x 500 meter region for 50 seconds of simulation time. All nodes have the same transmission range of 250 meters. However the proposed solution can be applied in any scenario. The simulated traffic is Constant Bit Rate (CBR). The simulation settings are given in **table 4.**

Table 4. Simulation Settings

No. of Nodes	50
Area Size	500 X 500
Mac	IEEE 802.11
Transmission Range	250m
Propagation Model	TwoRayGround
Network Interface	WirelessPhy
Antenna	OmniAntenna

In the simulation, attacks are simulated where the attacker nodes send bogus tickets to the nodes, which have requested for those tickets. These attacks can be isolated attacks where every attacker certifies a different public key. However, the attackers may also launch a cooperative attack where a group of attackers collude and send tickets for the same public key that is bogus. Both these types of attacks are simulated. The number of attackers is varied from 1 to 5. Both intra and inter operator movements are simulated along with the authentications.
The Simulation topology is shown in the following figure

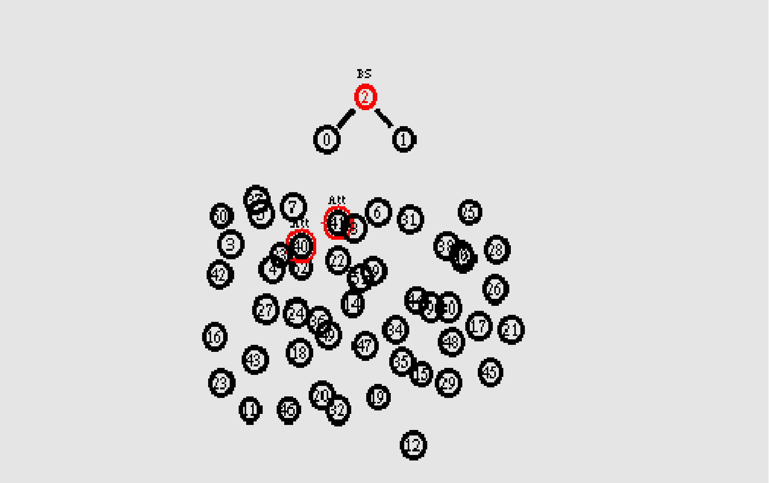

Fig. 5. Simulation Topology

4.2 Results

Both [5] and [6] are based on multi-operator wireless mesh networks. Since the proposed Trust Based Authentication and Key Establishment for Secure Routing (TBAKESR) protocol follows the same mutual authentication technique of [5], the proposed work is compared with the Authenticated Key Establishment (AKE) technique [6] for multi-operator wireless mesh networks. In order to evaluate the impact of the techniques at the receiver side, the packet drop and packet delivery ratio are measured. To analyze the impact of node capture attack, the fraction of compromised communications is measured. In order to evaluate the time complexity of the techniques, the latency is measured.

The authentication latency is measured for TBAKESR and AKE techniques. Fig. 6 shows the latency occurred of both the techniques when the number of attackers is increased. The latency increases as the number of attackers increases, since there will be more authentications to be performed. But TBAKESR has 38% lesser latency than AKE, since in TBAKESR router-to- router authentication is avoided.

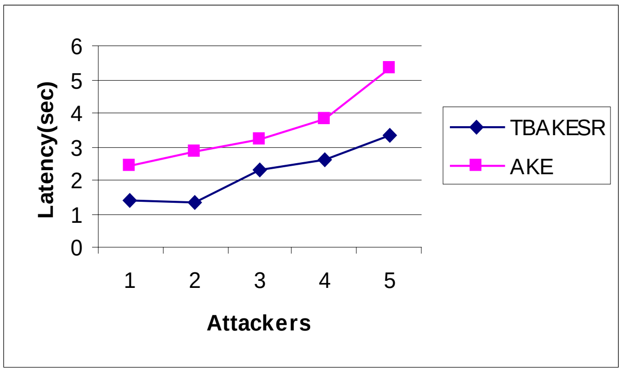

Fig. 6. Authentication Latency for Varying Attackers

The Packet Delivery Ratio is measured as the ratio of the number of packets received and the number of packets sent for both the techniques. Fig. 7 shows the packet delivery ratio of TBAKESR and AKE techniques when the attackers are increased. There is a degradation of delivery ratio beyond 3 attackers as seen from the figure. However, the delivery ratio TBAKESR 30% more than AKE, since it has trust authenticator on the top of hierarchy to verify the gateway and routers, thereby eliminating all possible attacks.

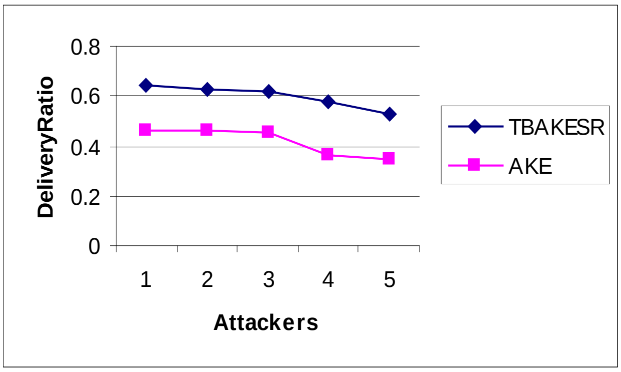

Fig. 7. Delivery Ratio for Varying Attackers

Next we measure the packet drop which refers the average number of packets dropped due to the attacks. Fig. 8 shows the packer drop occurred for TBAKESR and AKE techniques for different number of attacker scenario. The packet drop increases linearly, when the attackers are increased, as depicted by the figure. From the figure, we can see that TBAKESR has 64% lesser packet drops than AKE. This is due to the fact that TBAKESR uses trust authenticator on the top of hierarchy to verify the gateway and routers, thereby eliminating all possible attacks.

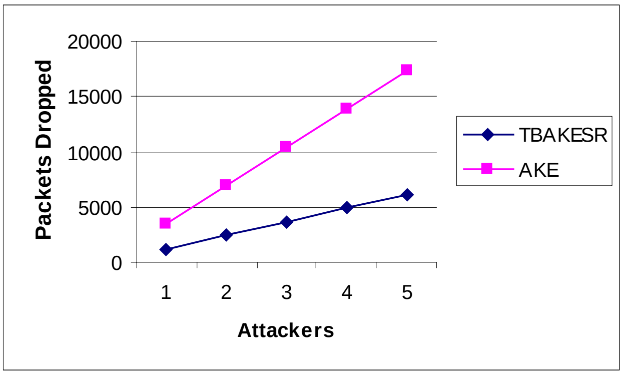

Fig. 8. Packet Drop for Varying Attackers

Next the fraction of compromised communications is calculated by estimating the fraction of communications compromised between non compromised nodes by a capture of x-nodes. **Fig. 9** shows the fraction of communication compromised for both the techniques. As it is seen from the figure, the compromised fraction for TBAKESR is 24% less when compared to AKE. This is because of the fact that, in TBAKESR, the attacker node's tickets will be expired quickly, since the expiration time is updated based on the estimated trust value.

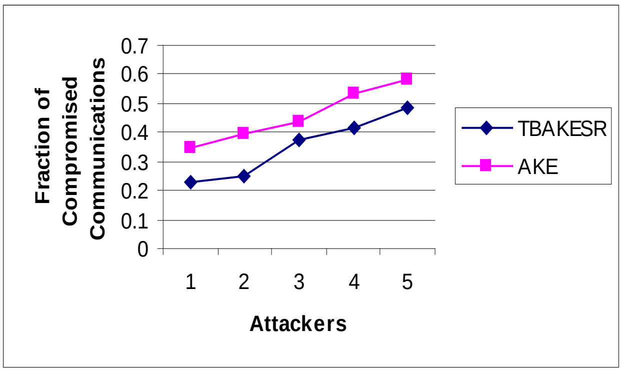

Fig. 9. Fraction of compromised communications for Varying Attackers

5. Conclusion

In this paper, we have proposed a trust based authentication and key establishment technique for secure routing in WMN. Initially, a trust model is designed based on ACO. This model involves exchanging of trust information among the nodes. The routing table is initialized for selecting the destination nodes, for which the link information is updated and the route verification is done. Based on the trust model, mutual authentication is applied. When a node moves from one operator to another for accessing router, then inter-authentication is performed. When the node moves within the operator for accessing the router, then intra-authentication is performed. During authentication, the keys are established using identity based cryptography technique. By simulation results, we have shown that the proposed technique enhances the packet delivery ratio and minimizes the packer drops due to attacks and fraction of compromised communications. As an extension to these works, we propose to design a privacy preserving (or) anonymity protection protocol for WMN.

References

[1] M.Jayanthi and .M.A.Mukunthan, "A Security Architecture for Implementing Anonymity and Traceability in Wireless Mesh Network using Clustering Concept," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 1, Issue-ETIC-2011, January, 2012.

[2] Celia Li, Zhuang Wang, and Cungang Yang, "Secure Routing for Wireless Mesh Networks," *International Journal of Network Security*, vol. 13, no. 2, pp. 109–120, Sept, 2011.

[3] Francesco Oliviero and Simon Pietro Romano, "A Reputation-based Metric for Secure Routing in Wireless Mesh Networks," *IEEE GLOBECOM*, 2008. Article (CrossRef Link)

[4] Shams Qazi, Yi Mu and Willy Susilo, "Securing Wireless Mesh Networks with Ticket-Based Authentication," in *Proc. of 2nd International Conference on Signal Processing and Communication Systems*, 2008. Article (CrossRef Link)

[5] Tianhan Gao, Nan Guo and Kangbin Yim, "Delegation-based Mutual Authentication Scheme for Multi-operator Wireless Mesh Network," in *Proc. of Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2012. Article (CrossRef Link)

[6] Bing He and Dharma P. Agrawal, "An Identity-based Authentication and Key Establishment Scheme for Multi-operator Maintained Wireless Mesh Networks," in *Proc. of 7th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, 2010. Article (CrossRef Link)

[7] Chen Dajun, Wang Chao and Lin Qiang, "Ant-Based Trusted Routing Algorithm for Wireless Mesh Networks," in *Proc. of Asia Pacific Conference on Postgraduate Research in Microelectronics & Electronics*, 2009. Article (CrossRef Link)

[8] Ramya R, Navamani T.M and Yogesh, "Secured Identity Based Routing and Privacy Preservation in Wireless Mesh Networks," *IEEE-International Conference on Recent Trends in Information Technology, ICRTIT* 2011. Article (CrossRef Link)

[9] Farah Kandah, Yashaswi Singh and Weiyi Zhang, "Mitigating Eavesdropping Attack Using Secure Key Management Scheme in Wireless Mesh Networks," *Journal of Communications*, vol. 7, no.8, 2012. Article (CrossRef Link)

[10] Tianhan Gao, Nan Guo, Kangbin Yim and Qingshan Li, "Anonymity Scheme with Unlink ability Property in Wireless Mesh Networks," in *Proc. of Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2013. Article (CrossRef Link)

[11] Xin Zhao, Yuqin Lv, Tet Hin Yeap and Bin Hou, "A Novel Authentication and Key Agreement Scheme for Wireless Mesh Networks," in *Proc. of Fifth International Joint Conference on* INC, IMS and IDC, 2009. Article (CrossRef Link)

[12] Jaydip Sen, "Secure and Privacy-Preserving Authentication Protocols for Wireless Mesh Networks," *Applied Cryptography and Network Security*. Article (CrossRef Link)

[13] Jaydip Sen, "Efficient Routing Anomaly Detection in Wireless Mesh Networks," in *Proc. of First International Conference on Integrated Intelligent Computing*, 978-0-7695-4152-5/10 $26.00 © IEEE, 2010. Article (CrossRef Link)

[14]Network Simulator: http:///www.isi.edu/nsnam/ns

G.Akilarasu received his B-Tech degree in Information Technology from Mahendra Engineering college under Anna University Chennai in 2006 and M.E in Computer Science and Engineering at Thiagarajar College of Engineering under Anna University of Tirunelveli in 2010 and He is Currently a Ph.D majored in Information and Communication Engineering at Thiagarajar College of Engineering. His current research interests are in the areas of Wireless Network Security,Wireless Mesh Networks.

S. Mercy Shalinie received her PhD in Computer Science and Engineering from Madurai Kamaraj University in 2000. She received her ME in Applied Electronics from Coimbatore Institute of Technology in 1991 and BE in Electronics and Instrumentation from Annamalai University in 1989. She is the Head of the Department of Computer Science and Engineering at Thiagarajar College of Engineering. She and her research scholars have published/ presented several research papers in journals and international/national conferences. Her current areas of interest include machine learning, neural networks and information security.