IJCTA, 9(23), 2016, pp. 241-246

Trust Based Secure Routing With Authentication for Wireless Mesh Networks

Parveen kumar Sharma* Rajiv Mahajan and Surender*****

Abstract : Secure routing is challenges in hybrid wireless mesh networks (WMNs). Researcher are trying to solve the problems of security, efficiency, deployment of nodes. Still problems present in integrity of reputation values with the authentication condition. This paper suggest a solution by issuing certificate to nodes using trusted third party server and hash algorithms for authentication . Trusted path is selected from different path having higher trust values .Proposed protocol TSRA is compared with CSROR by varying number of nodes.

Keywords : Trust table, packet counter, key generation, TTP.

1. INTRODUCTION

1.1. Wireless Mesh Networks

In the era of Internet World, Wireless Mesh Network is an emerging source of communication. Mesh routers are connected in such a way that they provide an environment for the client to be connected in the system at all the times. Mesh routers and gateways act as a backbone of WMN. Gateways are used to communicate with the external world by sending traffic from the client. Gateway nodes are connected to the wired structure. Each router transmits the packets to other nodes that are not within the range (*i.e.* direct communication). In addition, the gateway nodes can facilitate the incorporation of WMNs with the other wireless networks such as Wi-Fi, cellular networks and WiMax [1]. Mesh clients are smart phones, PDAs ,Tablet etc.

1.2. Types of WMNs

1. **Infrastructure/Backbone WMNs :** Mesh routers build an structure for clients by using several kinds of radio technologies. The main characteristic of WMN to be of self-organizing and self-restorative links by the use of mesh routers. By the use of gateway features, the mesh routers are linked to the Internet.
2. **Client WMNs :** Client mesh offers the peer-to-peer communication between the client nodes. In order to accomplish routing and design functionalities, the client nodes are clustered to form the actual network. In addition, client WMN offers end-user applications to the customers.
3. **Hybrid WMNs :** The arrangement of both infrastructure and client mesh forms a hybrid WMN. Mesh clients are capable to interact with the network to mesh routers and directly meshed with the other mesh nodes. This kind of structure offers connectivity to other webs.

2. RELATED WORK

Jin Ho Kim et al. **[6]** have suggested a secure multi-path routing protocol for WMN. It uses a hybrid routing protocol. The control overhead involved in the routing protocol is sufficiently reduced. It provides secure and reliable communication by discovering alternate routes.

* Research Scholar IGKPTU Jalandhar

** Professor GCET Gurdaspur

*** Assistant Professor GTB College Bhawanigarh (Sangrur), Pb

R. Matam et al. [9] have offered a (WRSR) to identify the wormhole attack by using route discovery process and isolate it. This algorithm identifies the direction necessities by negotiating a wormhole and avoids the creation of such routes. The unit disk graph is employed to decide the important and acceptable condition, and recognize the wormhole-free route. All forms of wormhole attacks can be easily detected and isolated without depending on any extra hardware. However, this algorithm has some packet loss because of the probable choice of wormhole nodes during early route finding.

Fahad T. Bin Muhaya et al. **[10]** have demonstrated the field based direction-finding which uses a minute facts for the direction the packets in the network. (ESFBR) is proposed a secure field routing process. This technique is presented with a confidence to secure the WMNs from internal and external attacks.

Young Yig Yoon et al. **[11]** have proposed SHWMP, a secure extension of Layer-2 routing stated in 802.11s that recognizes the mutable and non-mutable grounds in the routing note. By using the symmetric encryption, the non-mutable part is protected. Merkle-tree approach is used to validate the mutable information. This protocol is vigorous against known attacks and effective because of the symmetric key operations.

Celia Li et al. **[12]** have presented a security boosted AODV (SEAODV) routing protocol in which Blom's key pre-distribution system is used to start the pairwise key. Each node has two forms of keys, namely, PTK and GTK. PTK is used to achieve the distribution of GTK while GTK is used to safe transmission routing messages between the pair of node.

Francesco Oliviero et al. **[13]** have offered a new metric for routing in WMNs in which the author displayed how a reputation-based metric is realistic to the existing routing protocols and how this can increase the consistency of the network. AODV-REX is an addition to the AODV protocol that deeds a reputation metric to enhance the retreat level of the entire frame.

Shafiullah Khan et al. **[14]** have presented several aspects of the resource aware approach called CSROR protocol that depends on a cross-layer information give-and-take with some security contemplations. CSROR ensures the routing security and fulfills various presentations specific necessities for multimedia conveyance and real-time programs. Based on the several cross layer parameters, CSROR chooses an optimum route. Moreover, it is robust beside packet dropping attacks like black hole, grey hole and wormhole.

3. PROPOSED METHODOLOGY

3.1. Trust Initialization and updation

Proposed methodology uses Trust initialization and updation and Trust protection. To make invulnerable routing in Wireless Mesh Networks (WMNs) it uses trust tables and key management by trusted third party server. The TTP acts as trustworthy Documentation Rights (DR) server to release credentials to both APs and WMNs. The WMN or an AP get certificate from TTP . The digital signature are signed by TTP using its public key . The WMN needs to subscribe to the TTP straight or through its home AP to get the internet access. The TTP signs on WMN's new credential, and sends back to the WMNs. Nodes in the WMN communicate with other nodes while transmitting data packets from one end to another end.. Every node in the set-up resides of a trust table, trust counters are used for counting the value of adjacent nodes. Source node sends RREQ packets to its neighboring nodes. packet counter (PC) are used to count the number of packet forwarded to each path. TTP issues general key (GKey) and Pairwise secret key (PSKey) to each node. PSkey is secretly shared among adjacent nodes and GKey is normally shared among all adjacent nodes. Pskey has to be regenerated again when the nodes move from one position to another . keys will be refreshed at that times.

3.2. Trust Protection

(*a*) RREP message generation

When the RREQ message received destination node, it calculates the total packets successfully arrived (P_{rec}). For the Prec calculation we are going for the below algorithm.

```
Public void calculate (){
Static final int Prec = 0;
While (request. has Next)
{
Prec++;
}
}
```

Then it constructs the RREP message and sends towards the origin node in opposite direction. RREP message is constructed in two phases. In the phase1, hash value is generated after concatenation of P_{rec} and Gkey values. MD5 and SHA are two algorithms those generates hash function.

$$HV(G) = H1\ (Gkey \mid P_{rec}) \tag{1}$$

To provide secure routing, the second step is formulated,

(*b*) Hash key generation

During Phase2, by using SKey , hash value reproduced using the earlier one.

$$HV = H(SKey \mid H1) \tag{2}$$

Here, SKey denotes secret key of the destination.

H1 is the hash function.

HV hash value.

Finally, the source node id is added with the generated hash value. The final RREP message is transmitted from the destination point to the origin along the opposite route of RREQ message.

(*c*) Validation with messages

When the intermediate node n_i receives the RREP from another node n_j, along the reverse path, it validates it using its SKey first and then by Gkey. It then computes packet success ratio of n_j by,

$$PR_j = PCn_j / Prec \tag{3}$$

Then the TC value of node *j* is calculated as

$$TC_j = TC + PR_j \tag{4}$$

Where TC is the initial trust counter value.

(*d*) Refresh data generation

The node n_i then appends this TC value to the RREP packet, regenerate the hash value using its SKey and Gkey and forwards to the succeeding node in the opposite path. When the source node receives this packet, it validates the hash value and access TC value of all intermediate nodes.

Then to find trusted path, a trust value of path (PTV) is considered at the source node by adding all the TC values of nodes in the path.

(*e*) Trust path selection

The route having highest trusted path value is selected by source node

$$TP(C) = \max (TV_i) \tag{5}$$

Where $TP(c)$ = chosen trust counters

(TV_i) = each neighbor nodes Trust values where $i = 1,2,3 \ldots\ldots\ldots\ldots n$

Overall algorithm :

Step 1 : A network from source to destination is established through a number of nodes.

Step 2 : Proceed for trust initialization and updation phase.

Step 3 : Go for the trust protection for the network in a reverse manner.

Step 4 : Refresh the phases as given in step-2 and step-3.

4. EXPERTMENT AND RESULT

The Network Simulator (NS2) [15], is used to simulate TSRA with CSROR. In the simulation, the mobiles nodes are varying from 10 to 50 and in the of region (500x500) meter. Simulation time is considered as 50 second. Constant Bit Rate (CBR) is used as simulation traffic with in transmission area of 250 meter.

Table 1. Simulation parameter.

Number of Nodes	10, 20, 30, 40 and 50
Size of Area	500 × 500
Mac	IEEE 802.11
Series of Transmission	250m
Time of Simulation	50 sec
Source of Traffic	CBR
Size of Packet	512
Rate	50 kb
Variation of Attackers	1,2,3,4 and 5
wired Nodes	2
base stations	2

4.2. Performance Metrics

The proposed Trust Based Secure Routing with Authentication (TSRA) protocol is compared with the Cross Layer Secure and Resource-Aware On-Demand Routing (CSROR) [14] protocol. The performance is evaluated mainly, according to the following metrics.

- **Packet Delivery Ratio : T**he proportion between the quantity of packets accepted and the quantity of packets directed.
- **Packet Drop :** The difference between packet sent from source and packet received at destination.
- **Delay :** How much time spent by packet to reach from source nodes to the destination node.

4.3. Results

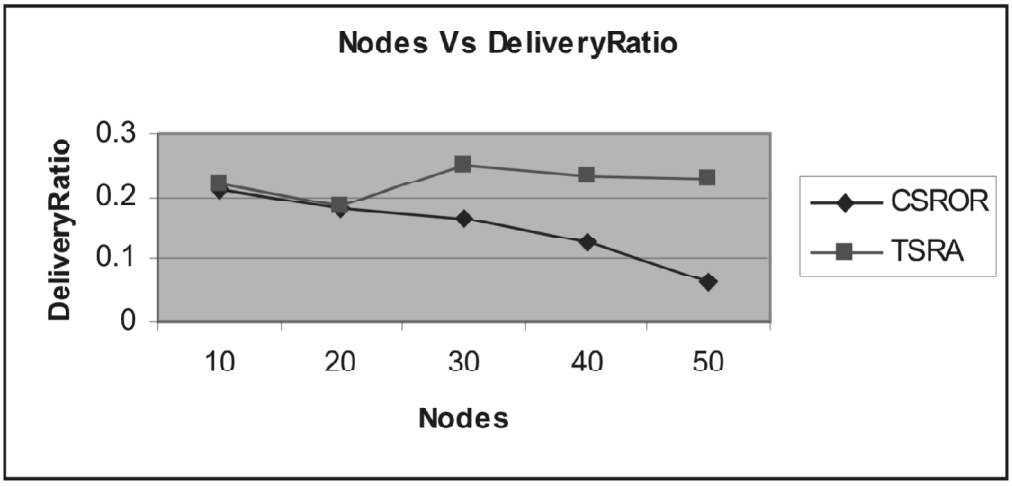

Fig. 3. Nodes Vs Delivery Ratio.

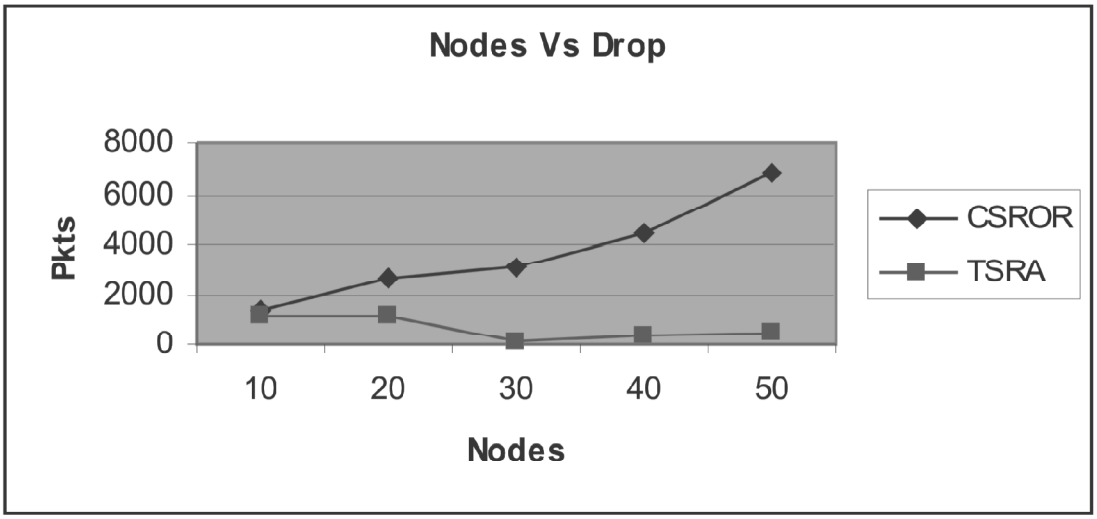

Fig. 4. Nodes Vs Drop.

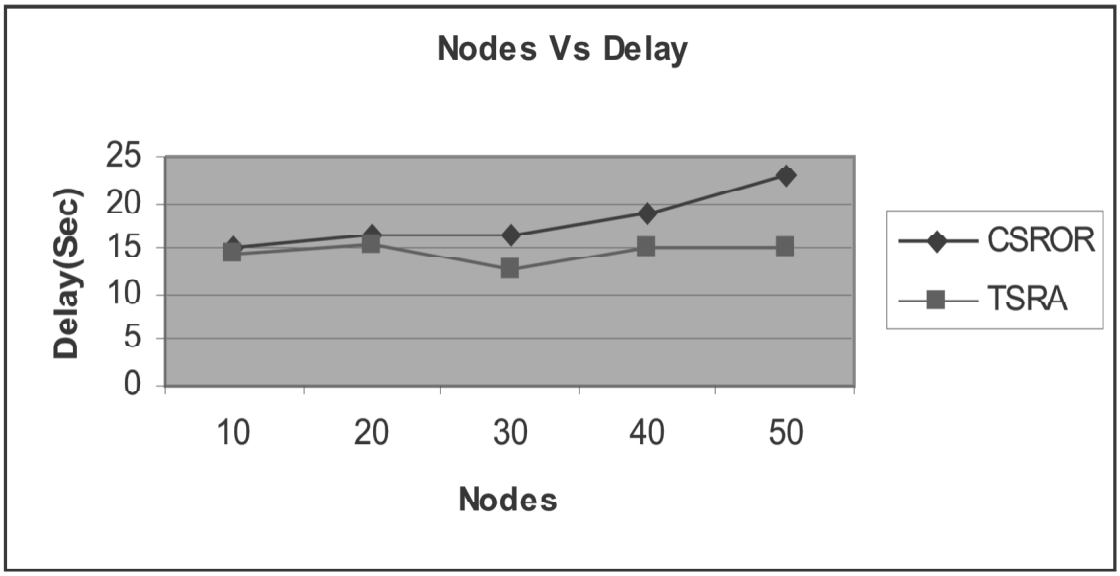

Fig. 5. Nodes Vs Delay.

Figure 3 illustrations of node vs delivery ratio of TSRA and CSROR by changing the quantity of nodes from 10 to 50. The delivery ratio of proposed TSRA approach has 31% higher than CSROR approach.

Figure 4 illustrations the node vs drop of TSRA and CSROR by changing the quantity of nodes from 10 to 50. The drop of our proposed TSRA approach has 71% less than CSROR approach.

Figure 5 illustrations of node vs delay of TSRA and CSROR by changing the quantity of nodes from 10 to 50. The delay of TSRA methodology has 17% less than CSROR methodology.

5. CONCLUSION

In view of integrity of reputation values with the authentication condition. Trusted third party server used for certification and hash generation for authentication of nodes . This is a complete solution for the authentication and authorization. By changing number of nodes Propsoed algorithm Trust base secure routing and Authentication protocol (TSRA) perform better when compared with CSROR by taking the parameter delay, packet drop and packet delivery ratio.

6. REFERENCES

1. Cristina Neves Fonseca and Instituto Superior Tecnico, "Multipath Routing for Wireless Mesh Networks",
2. Ian F.Akyildiz and Xudong Wang, "A Survey on Wireless Mesh Network", IEEE Radio Communication, 2005.
3. www.wikipedia.com
4. Muhammad Shoaib Siddiqui and Choong Seon Hong, "Security Issues in Wireless Mesh Networks", IEEE International Conference on Multimedia and Ubiquitous Engineering, 2007.
5. Yi Ping, Xing Hongkai, Wu Yue and Li Jianhua, "Security in Wireless Mesh Networks: Challenges and Solutions", Information Technology New Generations Sixth International Conference, pp-423-428, 2009.
6. Muhammad Shoaib Siddiqui, Syed Obaid Amin, Jin Ho Kim and Choong Seon Hong, "MHRP: A Secure Multi-Path Hybrid Routing Protocol for Wireless Mesh Network ", IEEE Military Communication Conference, 2007.
7. Anand Prabhu Subramanian and Milind M. Buddhikot, Scott Miller, "Interference Aware Routing in Multi Radio Wireless Mesh Network", 2nd IEEE Workshop on Wireless Mesh Network, pp-55-63, 2006.
8. Naouel Ben Salem and Jean-Pierre Hubaux, "Securing Wireless Mesh Networks", IEEE Wireless Communication, vol-13, pp-50-55, 2006.
9. Francesco Oliviero and Simon Pietro Romano, "A Reputation Based Metric for Secure Routing in Wireless Mesh Network", IEEE GLOBECOM, 2008.
10. Fahad T. Bin Muhaya1, Fazl-e-Hadi and Atif Naseer, "ESFBR- Enhanced secure field based routing in wireless mesh networks", Indian Journal of Science and Technology, 2011.
11. Md. Shariful Islam, Young Yig Yoon, Md. Abdul Hamid and Choong Seon Hong, "A Secure Hybrid Wireless Mesh Protocol for 802.11s Mesh Network "ICCSA, Vol-1, pp-972-985, 2008.
12. Celia Li, Zhuang Wang, and Cungang Yang, "Secure Routing For Wireless Mesh Networks", International Journal of Network Security, pp-109-120, 2011.
13. Francesco Oliviero and Simon Pietro Romano, "A Reputation Based Metric for Secure Routing in Wireless Mesh Network", IEEE GLOBECOM, 2008.
14. Shafiullah Khan and Jonathan Loo, "Cross Layer Secure and Resource Aware On Demand Routing Protocol for Hybrid Wireless Mesh Networks", Springer, 2010.
15. Network Simulator: http:///www.isi.edu/nsnam/ns