ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/96243, October 2016* ISSN (Online) : 0974-5645

Secure Authentication Framework Design and Routing Metric (SAF&RM) based Communication in Multi-Hop Wireless Mesh Networks

J. Srinivasan[1*] and S. Audithan[2]

[1]Department of Computer Science and Engineering, St. Peter's University, Chennai - 600054, Tamil Nadu, India; srinivasanstpeters@gmail.com
[2]Department of Computer Science and Engineering, PRIST University, Kumbakonam - 612501, Tamil Nadu, India; saudithan@gmail.com

Abstract

Objectives: This paper presents Secure Authentication Framework Design and Routing Metric based Communication in Multi-hop WMNs (SAF&RM). **Methods/Statistical Analysis:** In this paper, we use the PKC based pseudonyms that builds secure authentication framework with conditional privacy and Probabilistic Transmission Count (PTC) routing metric for improving reliable communications in WMN. **Findings:** The combination of MAC-layer retransmission-based reliability and link quality awareness effects are captured for designing the PTC. **Applications/Improvements:** This approach aims to diminish the sum of overall forwarding nodes in the routing and reduce the bandwidth consumption of the network which ensure high end-to-end packet delivery rate and improve the secure transmission in WMN.

Keywords: Pseudonyms, Probabilistic Transmission Count, Security, Trust Authority, Wireless Mesh Networks

1. Introduction

WMNs contain mesh routers and clients that are either mesh gateways or relays. Mesh clients are the terminal devices to which the WMN backbone provides connectivity; mesh relays are connected with each other by wireless links to form the network backbone; gateways represent a small fraction of routers that connect to the Internet. WMNs maintain multiple redundant communications paths, multi-hop routing, throughout of the network are usually present. [1]WMN essentially involves a careful choice of the installation's positions, an optimal choice of nodes, node interface assignment, superior conclusion on a judicious channel, while ensuring connectivity, coverage and communication at a minimum cost. Thus, the network automatically routes traffic through alternate paths if some links or nodes fail in the communication. Figure 1 shows the architecture of the WMN.

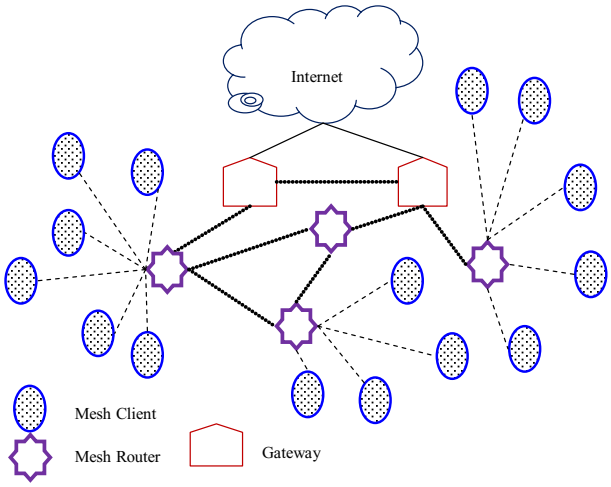

Figure 1. Architecture of the WMN.

However, when Quality of Service (QoS) is required, substitute paths will fail to re-route traffic towards gateways in the network. Therefore, reliability is considered as an

* *Author for correspondence*

important task. [2]The characteristics of WMN, such as the vulnerability of the wireless links, the limited physical protection of each node or the dynamically changing topology makes a challenge in providing the security to the network.

In WMN, for providing efficient security, authentication is essential. The goal of this paper is to offer an effective authentication and achieve high throughput in WMN. An efficient authentication framework was constructed by using the PKC based pseudonyms and ID-based key management with conditional privacy for communications in WMN. If an unauthenticated node transmits a fake authentication message, the trusted authority opens the corresponding signature for tracing the actual identity of the node. Design of a robust routing metric based on Probabilistic Transmission Count (PTC) can find high-performance paths in multi hop WMN.

[3]Multi-path hybrid routing protocol introduces multiple paths based on the graceful traffic splitting algorithms for balancing traffic over more than one path. This protocol dramatically grows the performance of the longer hop length flows of the network. The round robin scheduling increases the throughput of the network. [4]Secure Routing Protocol (SRP) utilized sequence number in the Route Requests (RREQs) and Route Replies (RREPs) to assure the novelty, but this sequence number can only be checked at the destination. The SRP needs a security involvement between the nodes that communicate with each other and applied this security concept to authenticate the RREQs and RREPs by Message Authentication Codes (MACs). This protocol can detect the alterations of the RREQs, modifications of the RREPs and assigns the route maintenance purpose of this protocol.

[5]Angle based Multicast Routing Algorithm (ARMA) reduces both the communication overhead and forwarding nodes in WMN. In this scheme, forwarding nodes are selected based on the node angle towards the destination direction. It improves the QoS in the network. [6]Fuzzy logic based link status classification mechanism discussed link status for multi-hop WMNs. Received Signal Strength (RSS), Node velocity and the distance between the neighbors nodes communicating in the network are taken as inputs. The status of the link is determined as the output. It predicts a particular link in advance, on the active path between the source and destination, break the links and reroute the operation thus minimizes the route discovery frequency, packet loss and delay.

[7]Probabilistic region failure model was used to catch a region failure and utilize it for reliability assessment in WMNs. The grid partition based scheme calculates the probable flow capacity degradation from a random region failure. The grid partition technique is for finding the susceptible partitions of a network. It offers network consistency under a region failure and help to design and maintenance of durability wireless networks.

[8]Two-level re-keying/re-routing scheme adapts a dynamic network topology and securely update keys for every data transmission. This scheme provides trustworthiness based on reliability and security. The reliability represents the capability to receive packets at a desired packet arrival success rate between 0 and 1. This protocol has low communication overhead. [9]Reliability Analytical Measurement (RAM) evaluates WMN reliability in planning phase. RAM is based on a model titled Multi Commodity Network Flow (MCNF) and Mixed integer Linear Programming (MLP) considers probabilities of node failures.

[10]In non-regenerative un-trusted relay network, the relay is a potential eavesdropper despite its assisting the source with cooperative transmission. Secrecy Outage Probability (SOP) and Connection Outage Probability (COP) are used to describe the level of reliability and security of the communication. The closed form of Reliable and Secure Probability (RSP) is derived to character the trade-off between reliability and security. The Monte-Carlo results verify the validity of theoretical analysis. [11]An integrated approach for reliability and dependability combines bandwidth management on the link layer, network coverage planning on the physical layer and live network monitoring to improve the reliability, availability and maintainability of a WMN. Fine-grained are used to improve the expectedness of the network components, thus making the WMN more dependable.

[12]Reliable Multicast in Multi-Rate WMN proposed Expected Multicast Transmission Time (EMTT) that decreases the amount of expected transmission time. EMTT is designed to capture the combined effects of MAC-layer retransmission-based reliability, transmission rate diversity, wireless broadcast advantage and link quality awareness. The Markov Decision Process (MDP) used to determine the optimal rate adaptation policy. The EMTT metric effectively reduces the overall multicast transmission time, provide higher packet delivery ratio and lesser end-to-end latency. [13]High-throughput reliable multicast in multi-hop WMN approach is a multicast routing metric known as Expected

Multicast Transmission Count (EMTX). The EMTX of single-hop transmit a multicast packet from a sender which is the expected number of multicast transmissions required for its next-hop recipients to receive the packet successfully. EMTX aims to reduce network bandwidth consumption while there is highest packet delivery ratio for the multicast traffic. [14]Dynamic programming approach computes Mesh Routing Algorithm (MRA) that provides the routing through more number of disjoint-link paths which includes the traffic through each path which is proportional to the capacity of the communication network. This approach compute high capacity and end-to-end delay bounded path. However, this approach does not offer the security in WMN. [15]Efficient bandwidth utilization with Congestion control (ECN) scheme reduces the congestion in WMNs. ECN scheme provides a sight of the actual state and increases the performance of a network.

[16]Throughput performance and fairness in multi-hop WMN (TP&F) can flexibly coordinate the tradeoff between throughput and fairness to adapt to different application based on rate adaptation algorithm, an adaptive capacity estimation algorithm and a queue management. In adaptation algorithm, nodes can dynamically change their rates according to the number of flows observed or to the updated rate overheard. In adaptive capacity estimation algorithm, nodes can adjust their rates by varying the fairness index provided that a certain fairness index threshold is satisfied. The queue management scheme enables nodes to transmit their data packets originated from different flows in a proportional manner. The rate adaptation and capacity estimation algorithms nodes can dynamically adjust their rates to maximize the throughput performance. The queue management scheme is used to guarantee fairness. However, this scheme does not provide any security algorithm in WMN.

The remaining contents of this paper include the following structures. The proposed model for SAF&RM in WMNs is presented in section 2. Section 3 provides the simulation analysis of SAF&RM. Section 3 conclude the paper.

2. Proposed Method

This section describes the design of the proposed authentication framework and routing metric based communication in multi-hop WMN. Router metrics can help to select the best route among the multiple routes from source to the destination. In this scheme, routing metrics can be designed based on the PTC. We invent the PTC objective of minimizing the sum of forwarding nodes in the routing and reduce the complexity of computing the metric. The trust authority and digital signatures design the authentication framework in WMN. Initially every node registers to Trusted Authority. Trust Authority generates the pseudonym to registered node based on the Public Key Cryptography (PKC). This pseudonym is used to identify privacy-preserving authentication and secure communication.

Trust Authority creates every node pseudonym as given below.

$$Ps = PK(id) \| T \| HD \tag{1}$$

Where

$T \rightarrow$ Current Time

$PK(id)$ Public key of node ID

$HD \rightarrow$ Code name of every node

The source broadcast the RREQ message to the communication range nodes. This RREQ message consist of this parameters such as

$$\langle ID_s, TS, HD, adv, nonce, SIG(ID_d, TS) \rangle \tag{2}$$

Where,

$ID_s \rightarrow$ ID of the source node

$TS \rightarrow$Timestamp

$HD \rightarrow$Codename of the node

$adv \rightarrow$Invite the node

$nonce \rightarrow$Freshness

$SIG(ID_d, TS) \rightarrow$Generate the signature of destination and Timestamp

Within communication range, nodes accept this RREQ message during the current time interval. Then these nodes send the RREP message to the source. RREP message contain

$$\langle ID_d, Ps, TS, join, SIG(Ps, TS), PTC \rangle \tag{3}$$

Where

$ID_d \rightarrow$ ID of destination

$Ps \rightarrow$Pseudonym generation

$join \rightarrow$Join request message

$SIG(Ps, TS) \rightarrow$Digital signature generated from the node pseudonym and the timestamp

$PTC \rightarrow$Predictable Transmission Count

The source receive the RREP message from these

nodes, the source verifies the signature and accept it, if the message is authenticated. If an unauthenticated node transmits a fake authentication message, the Trust Authority is able to open the representing signature to mark out the actual identity of the node. If the Trust Authority identifies any unauthenticated node, it sends a notification message to the all nodes.

2.1 Predictable Transmission Count (PTC)

The source node also checks the PTC. The PTC is defined as the MAC layer transmissions required in number that is required for delivering a packet through a wireless link successfully in the network. The PTC calculation is given in equation 4.

$$PTC = \sum_{m-1}^{\infty} mq^{m-1}(1-q) \tag{4}$$

Where

m → Transmission for node i to send data packet to the Node j successfully

q → Error Rate of the transmission

The PTC metric determines the outcome of packet loss ratios and length of the path.

The Figure 2 shows the architecture of the secure authentication framework. The mesh nodes are registered as the Trust Authority. The Trust Authority offers the nodes' real ID and pseudonym based on PKC. The source checks the communication range of authenticated nodes and its PTC. If the node is authenticated and the PTC rate is high, that node is selected as a next hop. This process is repeated until the source reaches the destination.

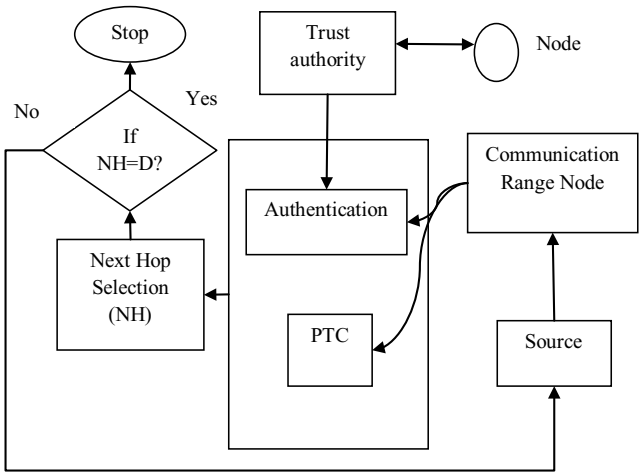

Figure 2. Working Strategy of Proposed Scheme.

3. Performance Evaluation

In this section, we provide performance evaluation of the SAF&RM which is performed by using the Network Simulator (NS2). This software is an open source programming language written in C++ and Object oriented Tool Command Language (OTCL). NS2 is a discrete event time driven simulator that is used to mainly model the network protocols. The nodes are distributed in the simulation environment. The simulation of the SAF&RM scheme is described in Table 1.

The simulation of the SAF&RM has 50 nodes deployed in the simulation area 1000×1000. The traffic is handled using the traffic model Constant Bit Rate (CBR). In this scheme, every node has the direct link with the nodes within the range 250m. The nodes are communicated with each other by using User Datagram Protocol (UDP). All the nodes receive the signal from all directions by using the omni-directional antenna. The performance of the SAF&RM scheme is analyzed by using the parameters Packet Delivery Rate (PDR), Packet Loss Rate (PLR), average delay, throughput and residual energy.

3.1 Packet Delivery Rate

The Packet Delivery Rate (PDR) is the rate of total packets delivered to all destinations to the total data packets sent by the source node in the communication network. PDR is measured by the equation 5.

$$PDR = \frac{\sum_{0}^{n} Packets\ Received}{Time} \tag{5}$$

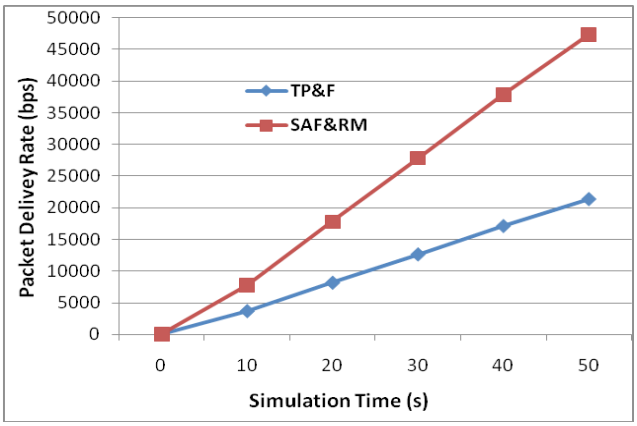

Figure 3. Packet Delivery Rate.

The Figure 3 refers the PDR of the SAF&RM is higher than the PDR of the TP&F.

3.2 Packet Loss Rate

The Packet Loss Rate (PLR) is defined as the difference between the sent packets and received packets in the network per unit time as in equation 6.

$$PLR = \frac{\sum_0^n Sent\ Pkts - Rcvd\ Pkts}{Time} \quad (6)$$

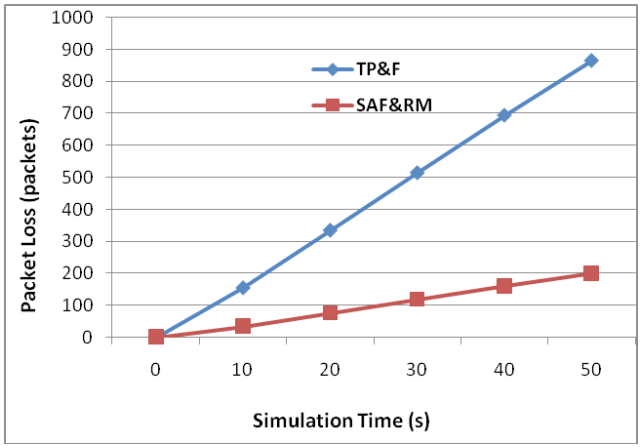

Figure 4. Packet Loss Rate.

Figure 4 indicates that the total packets lost of TP&F are greater when compared to the SAF&RM mechanism. The SAF&RM has reduced packets lost due to highest security routing.

3.3 Throughput

Throughput refers to the total number of packets successfully delivered across the network for every 1000 packets sent. Throughput is obtained using equation 7.

$$Throughput = \frac{\sum_0^n Packets\ Received(n) * Packet\ size}{1000} \quad (7)$$

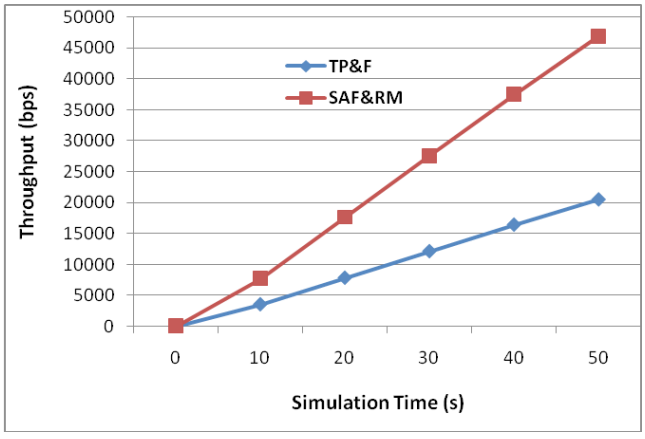

Figure 5. Throughput.

Figure 5 show that SAF&RM has greater average throughput when compared to the TP&F mechanism. The security activity has improved the network performance greatly.

3.4 Average Delay

The average delay is defined as the time difference between the current packets received and previous packets received. It is measured by the equation 8. Where n is the number of nodes.

$$Avg\_Delay = \frac{\sum_0^n (Packet\ \text{Re}ceived\ Time - Packet\ Sent\ Time)}{n} \quad (8)$$

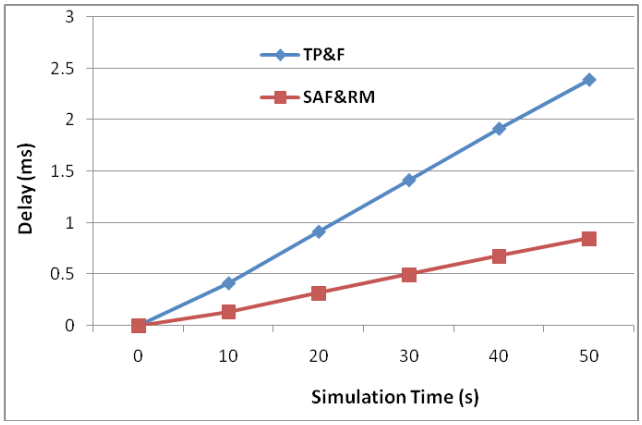

Figure 6. Delay.

The average delay value is plotted in Figure 6, which shows that the delay value is low for the proposed scheme SAF&RM than the existing scheme TP&F. The minimum value of delay means that higher value of the throughput of the network.

4. Conclusion

Secure Authentication Framework Design and Routing metric based Communication in Multi-Hop WMN (SAF&RM) achieves stable and reliable communication. In this paper, an efficient authentication framework is proposed with conditional privacy by using the PKC based pseudonyms and PTC for communications in WMNs. If an unauthenticated node transmits a fake authentication message, the TA should be able to open the representing signature to mark out the actual identity of the node. PTC robust routing metric can find high performance paths

in multi-hop WMN. This approach aims to minimize the sum of overall forwarding nodes in the routing and reduce the network bandwidth consumption. The simulation result ensure high end-to-end packet delivery rate and improve the secure transmission in WMN.

5. References

1. Benyamina D, Hafid A, Gendreau M. Wireless mesh networks design—A survey. IEEE Communications Surveys and Tutorials. 2012; 14(2):299–10.
2. Siddiqui MS, Seon C. Security issues in wireless mesh networks. IEEE International Conference on Multimedia and Ubiquitous Engineering, Seoul. 2007. p. 717–22.
3. Nandiraju NS, Nandiraju DS, Agrawal DP. Multipath routing in wireless mesh networks. IEEE International Conference on Mobile ad hoc and Sensor Systems, Vancouver, BC. 2006. p. 741–46.
4. Papadimitratos P, Haas ZJ. Secure route discovery of QoS-aware routing in ad hoc networks. Proceedings of IEEE Sarnoff Symposium Advances in Wired and Wireless Communication, Princeton, NJ. 2006; 176–79.
5. Thenral B, Thirunadana Sikamani K. AMRA: Angle based Multicast Routing Algorithm for Wireless Mesh Networks. Indian Journal of Science and Technology. 2015; 8(13):1–8.
6. Bianchi G. Performance analysis of the IEEE 802.11 distributed coordination function. IEEE Journal of Selection Areas Communication. 2000; 18(3):535–47.
7. Liu, J, Jiang, X, Nishiyama H, Kato N. Reliability Assessment for Wireless Mesh Networks Under Probabilistic Region Failure Model. IEEE Transactions on Vehicular Technology. 2011; 60(5):2253–64.
8. Hu F, Cao X, Kumar S, Sankar K. Trustworthiness in wireless sensor and actuator networks: towards low-complexity reliability and security. In IEEE Global Telecommunications Conference, Globecom'05. 2005; 3.
9. Beljadid A, Hafid A, Boushaba M. Reliability analytical measurement to design Wireless Mesh Networks. 2013 IEEE International Conference on Advanced Networks and Telecommunications Systems, (ANTS), Kattankulathur. 2013. p. 1–6.
10. Chen D, Wang L, Yin T, Xu X, Yang W, Cai Y, Yang W. Reliability and security performance analysis of non-regenerative untrusted relay networks. 2015 International Conference on Wireless Communications and Signal Processing, Nanjing. 2015. p. 1–5.
11. Lukas G, Herms A, Ivanov S, Nett E. An integrated approach for reliability and dependability of wireless mesh networks. IEEE International Symposium on Parallel and Distributed Processing, Miami FL. 2008; 1–8.
12. Zhao X, Guo J, Chou C T, Misra A, Jha S. A high-throughput routing metric for reliable multicast in multi-rate wireless mesh networks. Proceedings IEEE, Shanghai. 2011; 2042–50.
13. Zhao X, Guo J, Chou CT, Misra A, Sanjay K, Jha J. High-Throughput Reliable Multicast in Multi-Hop Wireless Mesh Networks. IEEE Transactions on Mobile Computing. 2015; 14(4):728–41.
14. Crichigno J, Khoury J, Wu MY, Shu W. A dynamic programming approach for routing in wireless mesh networks. IEEE Global Telecommunications Conference, Globecom'08, New Orleans, LO. 2008. p. 1–5.
15. Reddy CH, Gopal J, Sangaiah AK. Efficient bandwidth utilization with congestion control for wireless mesh networks. Indian Journal of Science and Technology. 2014; 7(11):1780–87.
16. Gao M, Jiang H. Throughput performance and fairness in multi hop wireless mesh networks. 2014 IEEE/CIC International Conference on Communications in China, Shanghai. 2014. p. 867–72.