An Authenticated Trust Based Security Mechanism for Video Transmission in Wireless Mesh Networks

J. B. Shajilin Loret[1], T. Ganesh Kumar[2]

[1] Department of Information Technology, Francis Xavier Engineering College, India
[2] School of Computing Science and Engineering, Galgotias University, India
shajilinphd@gmail.com, tganeshphd@yahoo.com

Abstract

Recently Wireless mesh networks (WMNs) have emerged as a key technology to meet the challenges in multimedia networks. Mostly the WMN are multi-hop in nature and in order to achieve availability, the routing protocols must be robust against both dynamically changing topology and malevolent attacks. In WMN, Security is one of the primary concerns due to the open nature and to ensure security in wireless mesh network (WMN) is a critical issue. To address the security vulnerabilities, though several secure routing protocols have been proposed but still there exist problems. In order to overcome this, a Secured Optimal Trusted Multipath Routing Protocol (SOTMRP) using fuzzy is proposed which is an extension of our previous work that improves the security in path selection. To ensure security in video transmission an Improved Dynamic DES algorithm (IDDES) is proposed and also to authenticate the destination an authenticated 3-way hand shaking mechanism is implemented in our system. The Simulation results show that the secured SOTMRP outperform well than other trust models by considering the various parameters such as Average throughput, Packet Delivery Ratio, Energy consumption, Trust value computation and Control Overhead.

Keywords: Wireless mesh networks, Secure routing, Trust value, IDDES, Fuzzy

1 Introduction

Wireless Mesh Networks (WMNs) have formulated as a promising technology in wireless environment. Wireless mesh networks (WMNs) are a multi-hop network and are dynamically self-configured and self-organized, with the network node which automatically represents an ad-hoc network and organizes the mesh connectivity [1]. WMNs are highly prone to various types of attack such as Denial of Service (DoS) attack and security attacks that occur in WMNs.

Though several security mechanisms such as cryptography, confidentiality, authentication and message integrity have been proposed to avoid security integrity have been proposed to avoid security threats such as snooping, message replay, and fabrication of messages, still these approaches suffer from many security vulnerabilities, which includes node capture attacks and denial-of-service (DoS) attacks. The outdated security mechanisms can able to resist only external attacks, but not the internal attacks effectively which are caused by the captured nodes to generate secure communications.

The most approaches indirect observation is used only to assess the nodes reliability, which are in out of the coverage range of the destination node [1-3]. In addition, most methods of trust evaluation from direct observation [2-4] do not differentiate data packets and control packets.

Integrated trust is evaluated by combining these two trust value such as direct trust (Gaussian probability) and indirect trust (Dempster-Shafer theory) and the probability value for each path is calculated based on the ELM algorithm. The probability value ranges between 0- 1. An improved version of Dynamic DES (IDDES) algorithm is used to deliver the data in more secured manner.

2 Related Work

Recently, several trust models have been developed by many researchers to build up trust relationships among wireless Mesh nodes [5]. Based on the behavior strategy banding D-S belief theory, one more related trust evaluation algorithm called as Node Behavioral strategies Banding belief theory of the Trust Evaluation algorithm (NBBTE) is proposed in [6].

In [7] an improved automated graph based DDoS attack detection mechanism based on Fuzzy Cognitive Map (FCM) on SDNs. A collection based routing protocol, called dynamic tree organizing routing (DTOR) [8]. A cloud user behaviour authentication model based on multi-label hyper-network [9].

A lightweight transparent authentication protocol named LHAP for adhoc networks is proposed in [10].

*Corresponding Author: J. B. Shajilin Loret; E-mail: shajilinphd@gmail.com
DOI: 10.53106/160792642021072204004

Wireless Sensor Networks (WSNs) play a crucial role in industrial IoT [11]. Workflow scheduling is one of the prominent issues in cloud computing [12].

In [13] A simple formula was designed to calculate vehicular total buffer size in these two cases, and to adjust the data flow to the receiver. ERASCA is secured from malicious/selfish attack through battery estimation technique [14].

By finding a secure end-to- end route for securing an adhoc network from independent malicious nodes. The trust-embedded AODV (T-AODV) routing protocol was designed in [15].

In order to solve the above problem, we propose an Optimized Weighted Trust Multipath Protocol to select multiple optimal trusted paths for enhancing the security in path selection from source to destination.

3 Proposed Method

The proposed Secured Optimal Trusted Multipath Routing Protocol (SOTMRP) is used to find the optimal trusted path between the source and destination in order to transmit the video frames. The input video is splitted into multiple 'n' sub streams and multiple optimal paths were used to transmit these sub streams. The optimal paths were identified using the weighted trust value of individual node. After finding the trusted paths Fuzzy inference system is used to select more optimal paths [16]. This SOTMRP is used for evaluating the trust weighted value between the mesh nodes by combining both direct and indirect method and can prevent security breaches more efficiently. For node authentication a 3 way hand shake mechanism [17] is used to avoid intruders.

3.1 Overview of SOTMRP

In this section, we describe the architecture of SOTMRP. When a source node wants to obtain the trust value of a destination node, both one hop trust model and multihop trust model is used. For this direct trust model is used or else the indirect trust model is used. The trust is calculated based on node B's direct experiences with node A in the direct trust model. Indirect trust model can be established when the source node A receives recommendations from other nodes about the Destination node B [16].

Trust be defined as a confidence level that whether a node can trust another node [18]. In this paper, the trust value is used to find if a node can perform normally in WMNs. Therefore the trust value is assumed to be in the range from 0 to 1 as in [19]. The node is taken as completely trustworthy if the trust value is between 0.6- 0.9 or 1, and that node can be avoided if it is between 0.1- 0.5 or 0. If a source node can communicate or transmit the data directly or without any intermediate nodes then it is called *direct trust* [20]. The indirect trust value is calculated based on the recommendations from other neighbouring nodes. By using the properties such as residual energy, communication, data content, inserted packet and multiplied packets the probability of the trust value is calculated to find the path trust value [21].

The overall block diagram is shown in Figure 1. In this paper the combination of both direct trust and indirect trust are used as in [20] to calculate the trustworthiness of mesh nodes. These paths were taken as input to the fuzzy decision making system to find the optimal path for transmitting the video frames.

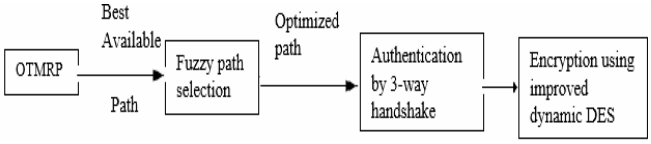

Figure 1. Over all block diagram of proposed work

3.2 Methodology

3.2.1 Computation of Trust value by Direct trust

In WMN the mesh nodes usually collaborate and communicate with neighbour nodes to perform their tasks. Generally, it is known that all communications in WMN will consume a certain amount of energy to transmit the data packets. Hence, the trust value for data content, residual energy, inserted packets, communication and multiplied packets are defined in SOTMRP.

The data content is used to find whether the data transmitted have reached the destination without any alteration. The data content is evaluated based on the packet drop ratio [21]. If the packet send by the source node is received correctly by the destination without any loss then the Packet dropping ratio is low. But if the packet received by the destination is less then it has the high Packet dropping rate.

The residual energy is used to measure if a mesh node is proficient in performing its intended functions or not. It is defined as the difference between total energy of the node to the energy used by the node. The residual energy p_m for a mesh node is considered to be in the range of 0-1. The residual energy p_m is calculated based on the consumption energy rate C_ε of a mesh node, where $C_\varepsilon \in [0, 1]$.

The communication is used to find whether the packets transmitted by a node have reached the destination correctly or to check whether the node is a selfish node, or replica node or malicious node. The trust value for the communication is considered as probability of the difference in the probability of packet received not occurring at time *t* [16].

The inserted packet is used to find the probability of number of packets inserted at time t. The trust value for the inserted packet can be calculated as probability of the difference in the probability of packet inserted not

occurring at time *t*. The trust values for the above properties using direct trust are computed as in [16].

In addition to this, multiplied packets are also considered in this paper. Multiplied packet is the number of packets multiplied by the node and the probability is evaluated based on the total number of packet multiplied. It is defined as the ratio between number of packet multiplied m_i in ith period of time where i varies between 1, 2, … n. to the total number of packet send. It is computed as

$$p_m = \frac{1}{\sqrt{2\sigma^2\pi}} e^{\frac{-(m_i-\mu)^2}{2\sigma^2}} \quad \textbf{(1)}$$

where p_m is the probability of packet multiplied. Therefore at time t the probability of packets multiplied are computed. The trust value for the multiplied packet can be calculated as difference in the probability of packet multiplied not occurring at time *t*. It is calculated as

$$\tau_m = (1 - P_m(t)) \quad \textbf{(2)}$$

Thus by using the above said parameters both the direct and indirect trust is evaluated.

3.2.2 Calculation of the Indirect Trust

Due to the malicious attacks evaluation of mesh nodes using only the direct trust is not accurate. Among the source and destination if the communication packets are higher than the threshold range the direct trust method is used [15] else there is a need of recommendations from the neighbours for the evaluation of trust. In multi-hop trust model, initially the source node needs to choose a set of neighbouring nodes and based on recommendation and trust propagation the indirect trust is evaluated.

The probability calculation for the indirect trust is evaluated by means of *Dempster-Shafer theory* as the concept in [22-23]. In order to make the trust more efficient and secure the distance metrics from neighbouring nodes and the appropriate trust values are considered by using *Evidence theory* [21]. For example when the source node S receives the recommendation from the neighbours, and if it receives different trust values, the difference value is measured as the trust value for that particular node. Then the weighted trust value is evaluated.

3.2.2.1 Probability of Indirect Trust Evaluation using Dempster-Shafer theory

Dempster-Shafer theory is used to evaluate the probability trust value using indirect trust method for each individual node as the concept in [22]. The belief function is the key part of this and is based on two key ideas which includes degrees of belief about a proposition which can be obtained from subjective probabilities of a related question, and these degrees of belief can be combined together on condition that they are from independence evidence [24-25]. Assume that there are more than one neighbor nodes between the source node and the destination node in the indirect observation.

3.2.2.2 Calculation of Distance Metrics From Neighbours Using Evidence Theory

The distance metrics from neighbour nodes are evaluated using the maximum voting strategy in Evidence theory for indirect trust calculation [16]. Assume that the probability value ranges between 0 - 1 and the threshold value is set as 0.5. if any metrics falls below the threshold Value that is not considered and assign it as 0. if the value is greater than the threshold then it has the max value and it is considered. Thus if it has the maximum voting strategy then the particular node is treated as the good node else it is taken as an intruder or an un authorised person.

3.2.2.3 Weighted trust value Calculation

The individual node weighted trust value is identified for finding the trust value for every path. The weighted value for each individual mesh node using direct trust is calculated by the summation of all the parameters which includes data content, residual energy, inserted packets, communication trust and multiplied packets.

The same process is used for indirect trust to find the weighted trust value. After the calculation of weighted trust value of individual nodes by both direct and indirect trust the average weighted trust value can be calculated.

3.2.2.4 Average Weighted value

Based on the node weighted trust value, the average weighted trust value for single path for both direct and indirect trust can be computed as in [16].

By this the average path trust value is identified and then by using the ELM the integrated trust evaluation is made. This technique is used to decide whether the particular path can be selected for data transmission or not.

3.2.3 Secure Path validation by ELM

In order to validate and to make decision about the secure path ELM is used. This ELM works based on three criteria which includes

- Normalization
- Weight Value identification
- Decision Function

Normalization is used to make a decision from the huge data set. We assumed that the trust value of normal node fall in the range of 0.6 to 0.9 or 1. To make the optimized high value each data is divided by the mean value. The weight value is considered as the decision value to make decision about whether the

node is a normal node or an abnormal node. Thus the trusted available paths were identified by means of ELM.

In the ELM algorithm the training set N consists of a set of trust value of both normal node and abnormal node. The mean value of the trusted nodes are taken as the centers. The hidden value is the decision value ie. For example, if the node value is 0.6 it can be taken as the trusted value 1. The hidden values are set for output weight and it is compared with each value. Finally, the output Matrix is evaluated.

3.2.4 Fuzzy Path Selection

Fuzzy inference system is used to optimize the path more efficiently as in [16]. Fuzzy control system encompasses the collection and encoding of human knowledge concerning prediction and classification, with applying the predefined rules for a given set of inputs [26]. The Optimal Path selection using Fuzzy Inference System is shown in the Figure 2.

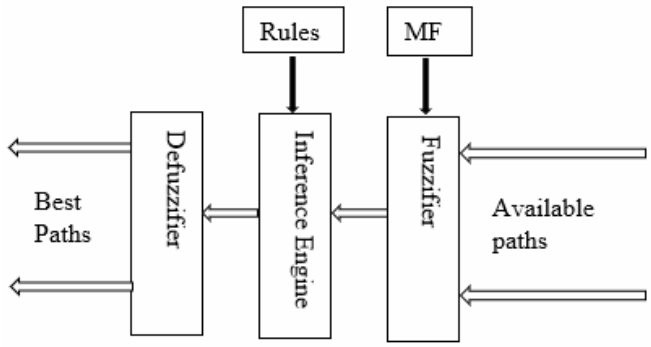

Figure 2. Optimal Path selection using Fuzzy Inference System

From the Figure 2 it is known that set of trusted available paths are given as input to the fuzzy inference system. The inference engine works based on the rules and fuzzifier output. The output of the inference engine is send to the defuzzifier to get the optimal best paths.

In addition to this, this paper also considers the node authentication and secure transmission. To authenticate the destination node an authenticated 3 way handshaking method is used as in [17] for transmitting the message. Also to provide security an enhanced version of DES namely Improved Dynamic DES (IDDES) algorithm is proposed.

3.2.5 Authentication

After the selection of optimal best paths and identification of destination node an authentication is provided by using authenticated 3 way handshaking methods before transmitting the data (message). This authentication is provided in order to avoid fake or false node. The encryption is done by using Improved Dynamic DES (IDDES) algorithm. The Figure 3 shows the authentication mechanism before transmitting the data.

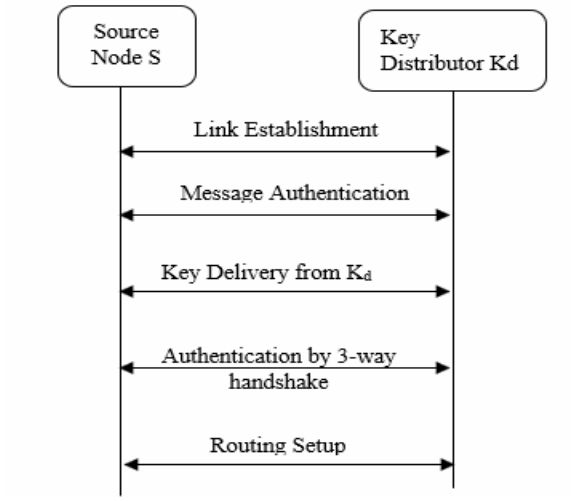

Figure 3. Authentication Mechanism

1. The peer link establishment is done between the Source Node *S* and the Key Distributer K_d.
2. Message authentication is done in using the HELLO Message.
3. The Key Distributer generates the key and it is delivered to the source node
4. An authenticated 3- way handshaking is done between the access point and the Source node for authentication.
5. Routing setup is done

3.2.5.1 An Authenticated 3 Way Handshaking

An authenticated 3 way handshaking method is used as in [17] to authenticate the destination node for transmitting the message. First the AP send a *HELLO* message to the Source node or user with it MAC address (*APA*), encrypted format of generated random value ($E_{PTK}[APnonce]$), Sequence ID (S_{ID},) and the message 1 (*MES1)* as *[APA,* $E_{PTK}[APnonce]$, S_{ID}, *MES1]*. Then the Source node generate a key and authenticate with the authenticator. If the received message is correct then the source node sends response message to the AP as (*SA,* S_{ID}, *Snonce, MES2*, MIC_{PTK}[Snonce, $S_{ID,}$ MES2]). Otherwise it generates new key to send the message to AP. Then the APverifies it and send back the response message to user by incrementing the sequence IDas (*APA,* S_{ID+1}, *Snonce, MES3,* $MIC_{PTK}[Snonce, S_{ID+1,} MES3]$). The Figure 4 shows the operation of an authenticated 3-way hand shaking.

3.2.5.2 Algorithm

Step 1. Receive the first Message from AP as [*APA,* $E_{PTK}[APnonce]$, S_{ID}, *MES1*]

Step 2. Source node decrypts the *[APnonce]* value and generates Snonce by calculating PTK to send Message 2.

Step 3. Message 2 received by AP

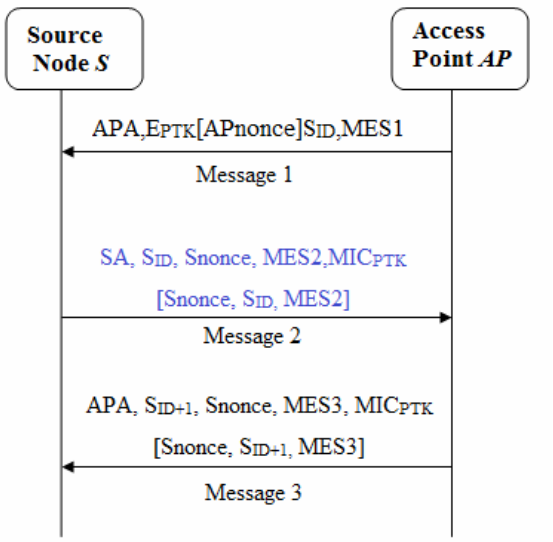

Figure 4. authenticated 3-Way hand shaking

Step 4. AP calculates PTK by using the same mechanism to Verify MIC and send Message 3.

Step 5. After receiving the Message 3, first the source node verifies and validates MIC.

3.2.6 Data Transmission by Improved Dynamic DES

After authenticating the destination node the data can be transmitted in a secure manner. So to provide security we proposed an enhanced version of DES namely Improved Dynamic DES (IDDES) algorithm. The IDDES is done by using 2 steps.

1. Signature Generation
2. Signature Verification

3.2.6.1 Signature Generation

In order to transmit the data from source to destination initially the Source node generates a dynamic secret key to encrypt the data. The encrypted message along with the secret key which is used for encrypting the message is signed by the source node before it forwarded to the destination. The generation of signature is shown below.

Generation algorithm:

Step 1: Select a dynamic key dk_s randomly, where $1 \le dk_s \le N-1$.

Step 2: Compute $x = A_s \bmod N$, where $(A_s) = df_s$. If x=0, go to step 1.

Step 3: Calculate the hash value $h_s \leftarrow h(m, r)$.

Step 4: Calculate $y = rdk_s h_s + dk_s \bmod N$ If y=0, go to step 2.

Step 5: The signature is the pair (x, y)

3.2.6.2 Signature Verification

After receiving the encrypted message, the destination node verifies the signature by means of signature verification algorithm. If the signature matches then the destination will decrypt the message. The signature verification algorithm is as follows.

Verification algorithm:

Step 1: Verify the signature pair (x, y) *and it is in the range of* [1, N-1]. If not the signature is invalid.

Step 2: Then compute the hash function as $h_s \leftarrow h(m, r)$

Step 3: Calculate $(A_s) = dk_s \bmod N$

Step 4: The signature is valid if $x = A_s$ mod N, else it is invalid.

Thus by using the IDDES algorithm the data can be transmitted securely using the optimized and secured path.

4 Performance Analysis

To examine the performance of the proposed OTMRP various simulation experiments are carried out. We implemented our proposed system in Network Simulator (NS2). The proposed system is compared with Optimal Link State Routing (OLSR), (HWMP), (SHWMP),(PA-SHWMP), Irregular Radio Model (IRM) and EWTMRP. The parameters used in the simulation experiments are listed in the below Table 1.

Table 1. Simulation Parameters

Parameters	Value
No of Nodes	50
Area Size	1000 x 1000
Target Size	[500, 500] × [500, 500]
Simulation Duration	600 sec
Queue Limit	20
Queue Size	100
Packet Size	552
Packet Interval	2
Communication Range	40 m
Buffer Size	25 packets

Several performance metrics are used for analyzing the performance the proposed method which includes Packet Delivery Ratio, Energy Consumption, Average throughput, Trust value computation and Control Overhead.

4.1 Packet Delivery Ratio (PDR)

Packet Delivery Ratio is an important metric used to analyze the network performance based on delivered packets. Packet Delivery Ratio is defined as the relation among the numbers of packets delivered correctly and the numbers of available packets. PDR is calculated by using the below formula

$$PDR = \frac{N_{pd}}{N_{pa}} \quad \textbf{(3)}$$

Where N_{pd} the total numbers of packets delivered is, N_{pa} is the total numbers of available packets. The

comparison graph for the packet delivery ratio is shown in the Figure 5.

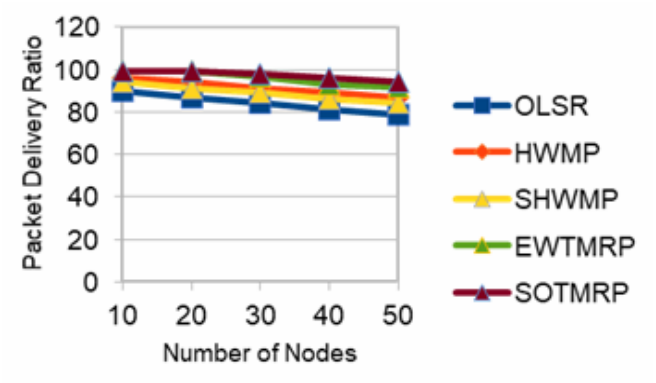

Figure 5. Performance analysis of Packet delivery Ratio

From the Figure 5 it is analysed that the packet delivery ratio of the proposed OTMRP increases with minimum number of nodes.

4.2 Energy Consumption

Energy consumption is the utilization of energy or power by each node. Generally, when there is increase in number of nodes the utilization of energy is also high. Our proposed system consumes less energy when it is compared with the existing protocols. The energy consumption graph of the proposed system is shown below in Figure 6.

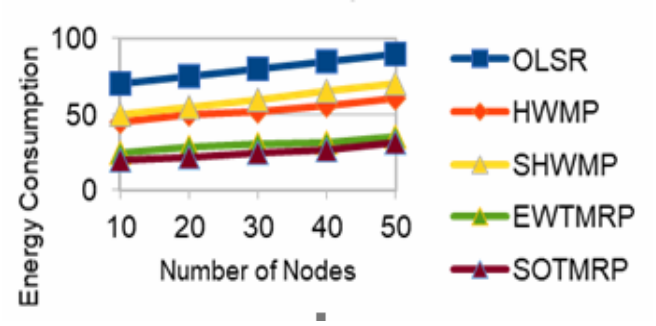

Figure 6. Performance analysis of Energy consumption

From the Figure 6 it is analysed that the energy consumption is gradually increasing when the number of nodes in the network increases. But when it is compared with the existing protocol the energy consumption is less and it gives better result.

4.3 Average Throughput (AT)

Average throughput is defined as the average successful message delivery rate over a communication channel. In general for the best system, the average throughput will be high while increasing the number of nodes. The throughput is high for our proposed system when it is compared with the existing protocols and it is calculated by using the below formula

$$T_{avg} = \frac{N_s}{N} \quad \textbf{(4)}$$

Where N_s the total number of packets is transmitted successfully and N is the total number of packets. The graph analysis is also shown below in Figure 7.

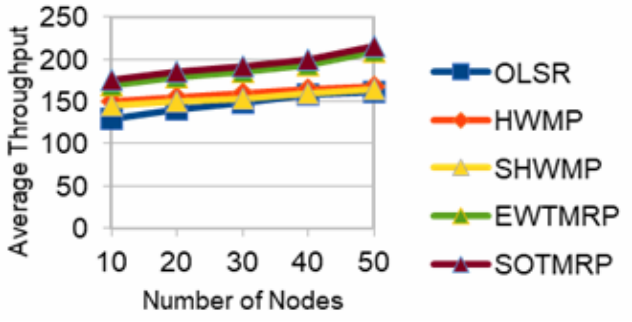

Figure 7. Performance analysis of Throughput Value

From the above Figure 7 it is examined that the proposed scheme gives better results when the number of nodes in the network increases.

4.4 Trust Value Computation

Trust value is computed based on the number of received packets. The variation between number of packets sent and number of packets received can be observed easily. These differences may be caused by addition of extra packets, modification of packets and loss of packets. The probability of packets that has been modified, added and lost can be computed by the following equation:

$$T_r = \frac{R_p}{T_p} \quad \textbf{(5)}$$

Where R_p is the remaining packets and is defined as $R_p = N_s - N_r$, N_s is the number of packets send, N_r is the number of packet received and T_p is the total number of packets. The performance analysis of the trust value calculation is shown in the Figure 8.

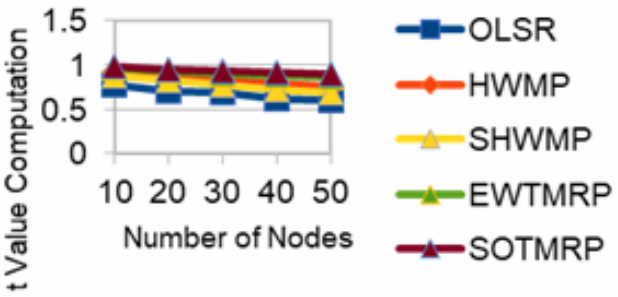

Figure 8. Performance analysis of Trust Value Computation

From the above Figure 8 it is observed that the trust value of the node is progressively decreasing when we increase the number of nodes in the network. When the proposed system is compared with the other existing protocols, it gives better results with high trust value.

4.5 Control Overhead

The major events in addressing a new protocol include initialization of network, adding a new node, deleting a node from the network and integration of nodes. In general these procedures, as well as the normal protocol operation, causes control overhead by reducing the available band width. The performance analysis of control overhead is shown in the Figure 9.

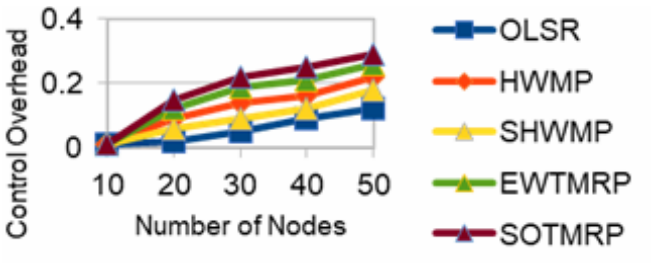

Figure 9. Performance analysis of Control Overhead

From the Figure 9 it is analyzed that while the number of nodes increases the control overhead also increases gradually and when comparing with other protocols it is very low. Thus it performs better and provides improved results.

5 Conclusions and Future Work

In WMN, an efficient trust model is essential for handling the trust related information in a secure and reliable way. In this paper, we extend our previous work Optimal Trusted Multipath Routing Protocol by providing authentication and secure communication. To provide security we proposed a Secure Optimal Trusted Multipath Routing Protocol (SOTMRP) which improves the security in path selection by integrating both direct as well as indirect trust. Also to ensure security in video transmission, an Improved Dynamic DES algorithm (IDDES) is proposed in WMNs. And an authenticated 3-way hand shaking mechanism is implemented to authenticate the destination node. The Simulation results show that SOTMRP outperform well by providing security than other similar trust models such as HWMP, SHWMP, PA-SHWMP, EWTMRP and OTMRP by considering the parameters Average throughput, PDR, Energy consumption, Trust value computation and Control Overhead.

References

[1] J. B. S. Loret, K. Vijayalakshmi, Fuzzy Based Multipath Routing over Wireless Mesh Networks for Video Transmission, *Australian Journal of Basic and Applied Sciences*, Vol. 9, No. 20, pp. 101-112, June, 2015.

[2] S. Buchegger, J.-Y. Le Boudec, *A robust reputation system for mobile ad-hoc networks*, EPFL IC Technical Report IC/2003/50, 2003.

[3] C. Zouridaki, B. L. Mark, M. Hejmo, R. K. Thomas, A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs, in *Proc of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'05)*, Alexandria, Virginia, USA, 2005, pp. 1-10.

[4] Y. L. Sun, W. Yu, Z. Han, K. J. R. Liu, Information theoretic framework of trust modeling and evaluation for ad hoc networks, *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, pp. 305-317, February, 2006.

[5] G. Han, J. Jiang, L. Shu, J. Niu, H.-C. Chao, Management and applications of trust in Wireless Sensor Networks: A survey, *Journal of Computer and System Sciences*, Vol. 80, No. 3, pp. 602-617, May, 2014.

[6] R. Feng, X. Xu, X. Zhou, J. Wan, A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory, *Sensors*, Vol. 11, No. 2, pp. 1345-1360, February, 2011.

[7] X. Li, Z. Fan, Y. Xiao, Q. Xu, W. Zhu, Improved Automated Graph and FCM Based DDoS Attack Detection Mechanism in Software Defined Networks, *Journal of Internet Technology*, Vol. 20, No. 7, pp. 2117-2127, December, 2019

[8] D. Kim, S. Kim, L. N. D. Triet, J. Cho, D. Ko, DTOR: Dynamic Tree Organizing Routing for Mobility Support in Wireless Sensor Networks, *Journal of Internet Technology*, Vol. 21, No. 4, pp. 1037-1048, July, 2020.

[9] R. Liu, X. Wang, J. Du, P. Xie, A Cloud User Behavior Authentication Model Based on Multi-label Hyper-network, *Journal of Internet Technology*, Vol. 20, No. 7, pp. 2071-2081, December, 2019.

[10] S. Zhu, S. Xu, S. Setia, S. Jajodia, LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks, In *23rd International Conference on Distributed Computing Systems Workshops*, Providence, RI, USA, 2003, pp. 749-755.

[11] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, K.-K. R. Choo, A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments, *Journal of Network and Computer Applications*, Vol. 103, pp. 194-204, February, 2018.

[12] M. Masdari, S. ValiKardan, Z. Shahi, S. Azar, Towards workflow scheduling in cloud computing: a comprehensive analysis, *Journal of Network and Computer Applications*, Vol. 66, pp. 64-82, May, 2016.

[13] H. Y. Kung, C. H. Chen, M. H. Lin, T. Y. Wu, Design of Seamless Handoff Control Based on Vehicular Streaming Communications, *Journal of Internet Technology*, Vol. 20, No. 7, pp. 2083-2097, December, 2019.

[14] F. Khan, A. W. Khan, S. Khan, I. Qasim, A. Habib, A Secure Core-Assisted Multicast Routing Protocol in Mobile Ad-Hoc Network, *Journal of Internet Technology*, Vol. 21, No. 2, pp. 375-383, March, 2020.

[15] A. Josang, An algebra for assessing trust in certification chains, in *Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99)*, San Diego, California, USA, 1999, pp. 1-10.

[16] J. B. S. Loret, K. Vijayalakshmi, Security Enrichment with Trust Multipath Routing and Key Management Approach in WMN, *Instution of Electronics and Tele Communication Engineers Journal of Research*, Vol. 64, No. 5, pp. 709-721, 2018.

[17] P. Singhal, M. Diwakar, M. Katre, Prevention of DoS and Memory Attacks: Enhanced 3-Way Handshake, *International Journal of Computer Applications*, Vol. 61, No. 3, pp. 31-35, January, 2013.

[18] J. Jiang, G. Han, F. Wang, L. Shu, M. Guizani, An efficient distributed trust model for wireless sensor networks, *IEEE transactions on parallel and distributed systems*, Vol. 26, No. 5, pp. 1228-1237, May, 2015.

[19] E. H. Mamdani, Application of fuzzy algorithms for control of simple dynamic plant, *Proceedings of the institution of electrical engineers*, Vol. 121, No. 12. pp. 1585-1588, December, 1974.

[20] N. Marchang, R. Datta, Light-weight trust-based routing protocol for mobile ad hoc networks, *Institution of Engineering and Technology Information Security*, Vol. 6, No. 2, pp. 77-83, June, 2012.

[21] K. Nordheimer, T. Schulze, D. Veit, Trustworthiness in networks: A simulation approach for approximating local trust and distrust values, in *IFIP International Conference on Trust Management*, Morioka, Japan, 2010, pp. 157-171.

[22] Z. Wei, H. Tang, F. R. Yu, M. Wang, P. Mason, Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning, *IEEE Transactions on Vehicular Technology*, Vol. 63, No. 9, pp. 4647-4658, November, 2014.

[23] N. J. Napoli, L. E. Barnes, A Dempster-Shafer Approach for Corrupted Electrocardiograms Signals, in *The Twenty-Ninth International Florida Artificial Intelligence Research Society Conference*, Key Largo, Florida, USA, 2016, pp. 355-360.

[24] G. Shafer, J. Pearl, *Readings in uncertain reasoning*, Morgan Kaufmann Publishers Inc., 1990.

[25] T. M. Chen, V. Venkataramanan, Dempster-shafer theory for intrusion detection in ad hoc networks, *IEEE Internet Computing*, Vol. 9, No. 6, pp. 35-41, November-December, 2005.

[26] W. Siler, J. J. Buckley, *Fuzzy expert systems and fuzzy reasoning*, John Wiley & Sons, 2005.

Biographies

J. B. Shajilin Loret works as Associate Professor at the Department of Information Technology, Francis Xavier Engineering College, Tirunelveli, India. She received her BTech degree in Information Technology from Anna University Chennai and MTech degree under Manonmaniam Sundaranar University. She has completed her research in Wireless Mesh Network at Anna University Chennai. She has published many Indian Patents. She has published many SCI and Scopus Indexed Journals. Her area of interest includes Network Security, Medical Imaging and Wireless Networks.

T. Ganesh Kumar received his Master of Engineering in Computer Science and Engineering from Manonmaniam Sundaranar University, Tirunelveli, India. He has completed Fulltime PhD in Computer Science and Engineering in Department of Computer Science and Engineering from Manonmaniam Sundaranar University, Tirunelveli in the year of 2016. Currently He is working as an Associate Professor in School of Computing Science & Engineering, Galgotias University, Greater Noida, Delhi NCR, India. He has published many SCI and Scopus Indexed Journals. He has published many Indian patents and international patents. His area of interest includes Computer Networks, Remote Sensing and Medical Imaging.