STMR - Secure Token Based Multipath Routing Protocol for Manets Using Hybrid Clustering and Path Selection Algorithm

S. J. Sultanuddin, Mohammed Ali Hussain

Abstract: Manet, security is unsolvable problem for recent developed and high density environments. A secure token based multipath routing (STMR) protocolis proposed for MANET using hybrid clustering and path selection algorithm. In STMR, cluster formation is performed by the Triangle optimization algorithm with the balanced set. The cluster head (CH) is selected by the trust degree calculate by performance metrics are energy consumption, received signal strength, mobility, congestion rate, cooperation rate and network lifetime. Then, an optimal path is compute by the multi-favor decision making algorithm, which selects the better path among multiples. Finally, the STMR protocol is applied to AOMDV to verify/evaluate the performance.

Keywords: mobile ad hoc networks (MANET), secure token based multipath routing (STMR), cluster head (CH), AOMDV, clustering.

I. INTRODUCTION

In recent times, development of wireless technology and growing popularity of wireless devices produced wireless networks so famous. [1] is infrastructure-less network comprising of set of wireless nodes that communicate with one another over one or more connections. The various attacks possible to affects the routing protocols performance, mainly, wormhole, black hole, Sybil and rushing attack [2]. The attacks on routing protocols, the malicious or compromised nodes can alter the sequence number and routing information in the packet. [3] Builds the matrix traffics from one point to another point by utilizing the time slicing method, and then achieves the end-to-end traffic matrix includes a group of traffic filtering rules. An authenticated anonymous secure routing (AASR) [4] is utilized to upgrade the necessities and improve the performance. QoS aware secured end to end data communication (QASEC) has utilized to choose transmission link to preserve a sensible data transmitted between destination nodes to source nodes [5]. Proficient hybrid protocol offers an effective route discovery approach together with a competent three-fish algorithm with neighboring clusters and effectively utilizing this information to decrease the routing overhead in clustered enhanced adaptive acknowledgement MANETs. At last, the anomaly in the network is identified by utilizing the SVM classifier [6]. Secure and effective random paths selection algorithm offers solution for number of the attacks.

II. CONTRIBUTION

A secure token based multipath routing (STMR) protocol is proposed using hybrid clustering and path selection algorithm. The standard AOMDV act as the base to test the new STMR protocol. The ain objective of proposed STMR protocol is proved ecure routing without affecting performance. The remaining part of work is discussed in section wise. Section 2 explanation of literature work. Section 3 describes the information about AOMDV-STMR protocol. The detail description model is explained in Section4. The performance analysis and results of AOMDV–STMRis illustrates in Section5. Finally, the paper concludes in Section6

III. RELATED WORK

In paper [8] a fuzzy logic based greedy routing-protocol is proposed for VANET. The protocol will give high security to the VANET. The security is an important factor in the VANET because the nodes in the VANET are moving faster that nodes in other networks.

In paper [9] a protocol that is used in the military or rescue operation in which frequent recharging of the energy source is not possible. EA-AOMDV is used to extend the lifetime of the battery; this will helps the network to operate long period of time.

In paper [10] due to the absences of the base station and nodes in MANET will force neighborhood node to send the message; this will make the MANET to be untrusted network.

In paper [11] a secured AODV protocol is proposed in order to identify and remove the black hole and grayhole attacks. Due to the open nature and lack of infrastructure of the MANET the security of the network is an important factor.

In paper [12] a hybrid encryption scheme is used to improve the security. MANET is a wireless network with movable infrastructure attacks are wormhole, packet dropping, jelly fish, black hole attack may affect the network.

In paper [13] proposes EAACK protocol to solve the issues like packet drops. It also proposes a hybrid cryptography techniques DES to decrease the overhead packet delivery ration. In paper [14] proposes an approach uses

Revised Manuscript Received on April 07, 2019.

SJ SULTANUDDIN Computer Science and Engineering, Sathyabama Institute of Science and Technology, Sathyabama University, Chennai, India.

Dr. MOHAMMED ALI HUSSAIN, Elecronics Computer Management, KL Deemed to be University, Guntur, Andhra Pradesh,India

Third Author name, His Department Name, University/ College/ Organization Name, City Name, Country Name.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

RSA and AES algorithm along with SHA 256 Hashing technique. The approach gives data authentication. Enhanced adaptive acknowledgement is the technique used to find the malicious node present in the network.

IV. PROBLEM METHODOLOGY AND NETWORKED MODEL

A. PROBLEM METHODOLOGY

Borkar et al. [16] has predicted the stable multi-cast distance for transmitting multimedia-data in MANET by utilizing proposed Multi-path Routing Scheme (MRS). A multi-path network is built and the transmission route will establish in two phases. From [8]-[16], still the security is unfixable issue for modern designed and high density mobile surroundings. Moreover, improvement in MANET’s security, we propose secure token based multipath routing (STMR) protocol for MANET. The major contributions of proposed STMR protocol are recapitulated as follows:

- In STMR protocol, the triangle optimization technique used to make a cluster with the improvement of balanced set.
- CH node is chosen by the trust degree depending on the performance metrics includes mobility, cooperation rate, network lifetime, congestion rate energy consumption and achieved signal strength
- The enhanced optimal path is compute by the multi-favor decision making algorithm, which chooses enhanced path among multiple paths between two CHs.
- STMR protocol is fed to AOMDV to performance evaluation. NS2 simulation outcome confirms the improvement of proposed protocol in terms of transmit energy, output, channel load, packet delivery ratio, BER, and buffer occupancy

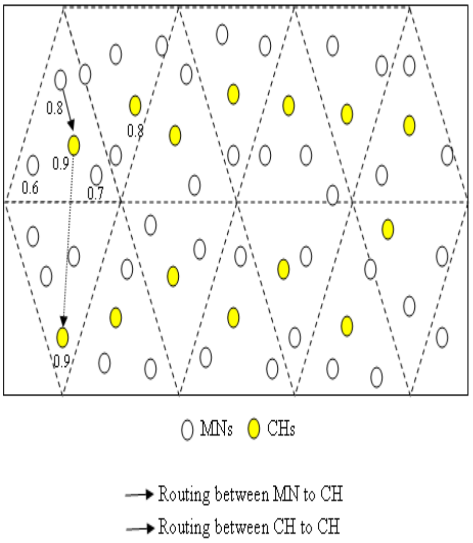


Fig. 1 Network model of proposed STMR protocol

B. NETWORKED MODEL

STMR protocol is represented in Fig. 1, it comprises of cluster head nodes (CHs) and mobile nodes (MNs). Base station (BS) utilized to gather the information from the mobile nodes. Primarily, MNs are arbitrarily distributed in the network. Subsequent to formation of cluster, we have to calculate the trust degree of each node utilizing some groups of metrics. The greatest trust degree node is work as CH among multiple nodes in the cluster. CH is accountable to collect data information from cluster components and more promote to sink/BS in the network.

V. SECURITY TOKEN BASED MULTIPATHROUTING (STRM) PROTOCOL

In the proposed protocol two approaches like hybrid clustering and path selection algorithm are used to enhance the performance of the MANET. Two parameters like cluster formation and the cluster header are taken into consideration. Triangle optimization algorithm is used for the cluster formation. The trust degree value is used to select the CH. After that the optimized path should be identified, in order to find the path the multi-favor decision making algorithm is used.

A. CLUSTER FORMATION USING TRAINGLE OPTIMIZATION ALGORITHM

The network is divided into clusters using the triangle optimization algorithm. The clusters which are located equal distance to the BS will have equal sizes. This method will increase the lifetime of CH. The increased lifetime of the cluster will helps to maintain the connection with in the structure. It also balances the energy consumed between the nodes. to model the network the graph modeling is used. Consider a graph G = (V, E) in which the V is the set of sensor and E is the wireless connections between nodes and is given by

$$E = \{(\mathrm{u}, \mathrm{v}) \subset \mathrm{V/D}\ (\mathrm{u}, \mathrm{v}) \leq R\} \qquad (1)$$

In order to find the energy consumption the parameters like packet/frame loss ratio and packet/frame forward energy are considered. The ratio of lost packets in receiver side to the whole number of packets sent form transmitter. The amount of data and the distance that is send from the source is used for calculating the energy consumption in terms of FFE. When the propagation distance is less than the threshold then the energy consumption is proportional to square of distance otherwise it is proportional to the square of distance. Therefore total energy consumption is given by:

$$E_{total} = FER(n, d) + FRE(n) \qquad (2)$$

Similarly, the total energy consumption will depends on three parameters like

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

communication unit, sensing unit and the processing unit.

$$E_c(u) = E_{c/comm}(u) \qquad (3)$$

$E_c(u)$ is the energy consumed by the node u. Then, in communication unit, energy consumption is given by:

$$E_c(u) = E_{Tx}(k,d) + E_{Rx}(k) \qquad (4)$$

Algorithm 1 Cluster formation

```
Initialize the count to 4
Initialize j as 0 < j ≤ 100
    if (j > 1000)
        cluster occur in 4 triangles
    end
    if (j > 1000)
        count++
        for the first triangle
            i = i/4
    end
```

Return Cluster formation

The equation of the E_{Tx} and E_{Rx} is given by:

$$E_{Tx}(k,d) = E_{elec} \times k + \in_{amp} \times k \times d^{\lambda} \qquad (5)$$

$$E_{Rx}(k) = E_{elec} \times k \qquad (6)$$

The working function of proposed cluster formation is given in Algorithm 1.

B. CLUSTER HEAD SELECTION

The CH is selected according to the trusted degree value. The node which is having the highest trusted value selects CH. The CH of one cluster can communicate with other clusters. After a selection of cluster-head the formation of path is next step. For the path formation the multi-favor decision algorithm is used. The path selected should be an optimized one. The data are transferred by making the connection between nodes having highest trusted degree.

Algorithm 2 CH selection

```
Initialize the an array of n variable
 while (a!= n×n)
 {
     for (I = 1; I<= n; I++)
     for (J =1; J<= n; J++)
        if (I > J)
           CH = I;
        else
           CH = J;
           I = J;
           a = a+ 1;
 }
        end
 End
```

Return CH node

Depending on all the above mention condition the trust values are calculated for every node. Then, the depending on those values the CHs are assigned for each cluster. Finally, the trust value (T_v) is written as follows:

$$T_v = \text{Avg}\,(E_c\,,\ \text{RSS, FLR, FFE, ROH}) \qquad (7)$$

The working function of proposed CH selection is given in Algorithm 2.

C. PATH SELECTION USING MULTI FAVOR DECISION MAKING ALOGIRTHM

Multi favor decision making MFDM is used to solve decision and planning that involves multiple criteria. A non-dominated solution states that least one criterion should be solved otherwise it is not possible to other solution. Hence, the decider can choose a solution from the non-dominated set. Otherwise, the decider could not do any worse of them and could do better in terms of all the criteria. However, the sets of non-dominated solutions is too larger enough to present to the decision maker for their final choice. The Fuzzy-logic based decision making algorithm is used to make the solution for various situations. Using the fuzzy decision making more accurate decision can be obtained.

Algorithm 3 Path selection

```
Initialize i as the first of clusters
Initialize j as the second of clusters
 for (i = 1; i <= n; i++)
   for (j = 1; j <= n; j++)
   {
     if( a[i] > a[j] )
      {
        Temp = a[i]
        a[i] = a[j]
        a[j] = temp
      }
   {
     end
```

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Return CH node

By using MFDM strong decision can be taken. It also find an alternative in case of complex situations. A fuzzy multi criteria decision-making technique is used to make the decisions. If non fuzzy methods are used for the decision making the performance will be degraded. Lorenz's description can be changed into the following fuzzy rules:

$$\text{if near}_i(x^i, c^i) \text{ then wi} = +1$$

$$\text{if far}_i(x^i, c^i) \text{ then wi} = -1$$

Where i is the state variable, xi(t) is the location, wi(t) is the fighting inclination and ci(t) indicate the next location. xj also indicate the location of near nodes. The member functions of the fuzzy logic as follows:

$$n_i(x, y) = \exp(-\|x - y\|^2/k_i^2) \qquad (8)$$

neari(x, y) can be determined by using the member function ni(x, y), ki determines thespread of the Gaussian function. The working function of proposed path selection is given in Algorithm 3.

VI. SIMULATION RESULTS

The progress of STMR protocol is derived under different network scenarios. The performance of STMR protocol is suited with AOMDV–SAPTV protocol.

A. SIMULATION SETUP

The STMR protocol is obtained from Network Simulator (NS2) tool with software platform of Ubuntu 12.04.For this test, the mobile nodes are randomly deployed in network area as 100×100 m2. The transmission of mobile nodes is 25 m. All nodes has battery power 18,720 J. The bandwidth of mobile node is 10Mbps. The average data packet size is 1024 bytes. IEEE 802.15.4 MAC protocol is used. The average speed of mobile node is 10 m/s. The simulation needs 1000 seconds to evaluate entire testing scenarios. The performance is evaluated by two different testing scenarios are: varying number of nodes and varying number of attack nodes. The performance of STMR protocol is matched with AOMDV–SAPTV protocol to check the Graph results..The simulation parameters and test scenarios were used in our simulation are listed in Table 1 and 2 respectively.

Table 1 Simulation parameters

Parameters	**Values**
Network area	100 × 100 m^2
Number of mobile nodes	20, 40, 60, 80 and 100
Average speed of mobile nodes	10 m/s
Number of attack nodes	2, 4, 6, 8 and 10
Initial battery power	18,720 J
Transmission range	25 m
Traffic source	CBR
Data packet size	1024 bytes
MAC protocol	IEEE 802.15.4
Simulation time	100 s

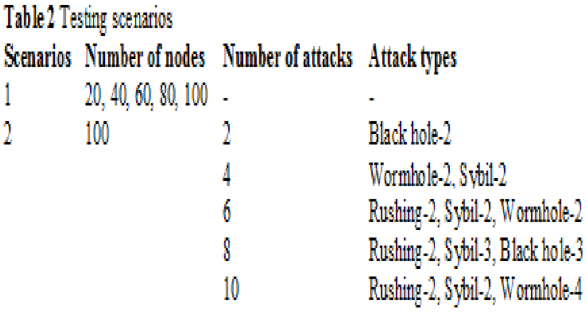
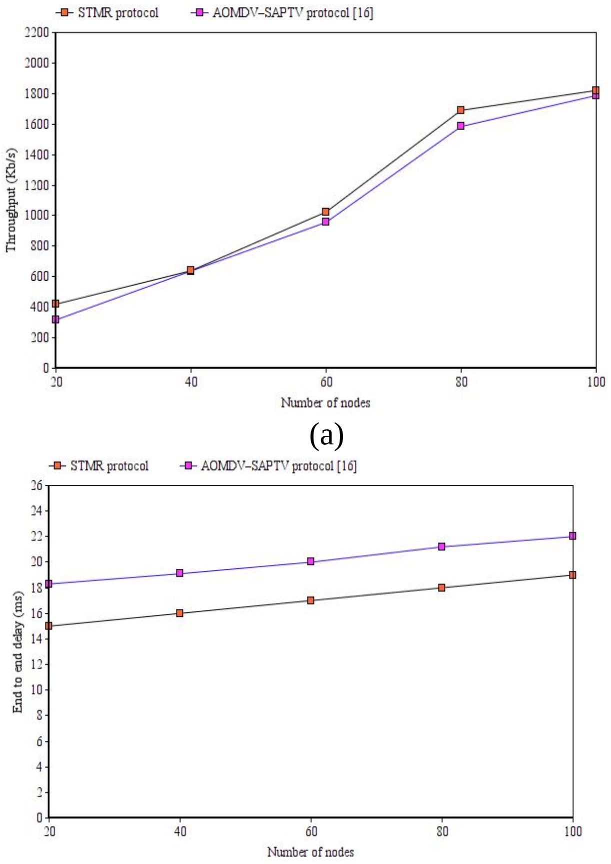


Table 2 Testing scenarios

Scenarios	Number of nodes	Number of attacks	Attack types
1	20, 40, 60, 80, 100	-	-
2	100	2	Black hole-2
		4	Wormhole-2, Sybil-2
		6	Rushing-2, Sybil-2, Wormhole-2
		8	Rushing-2, Sybil-3, Black hole-3
		10	Rushing-2, Sybil-2, Wormhole-4

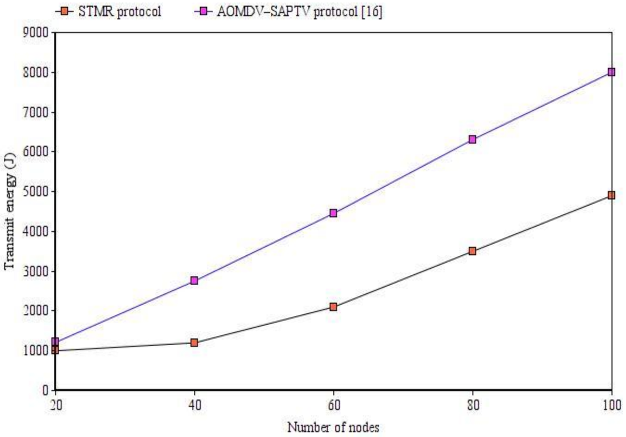
B. VARYING NUMBER OF NODES

In this test, varying the number of mobiles node from 20 to 100 in the fixed network area. The performance comparison of proposed STMR and existing AOMDV–SAPTV protocol is given in Fig. 2a-g. The plots clearly show the performance of various graphs.

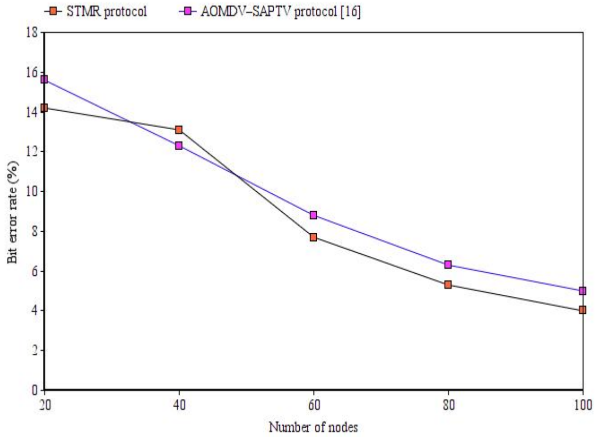


(a)

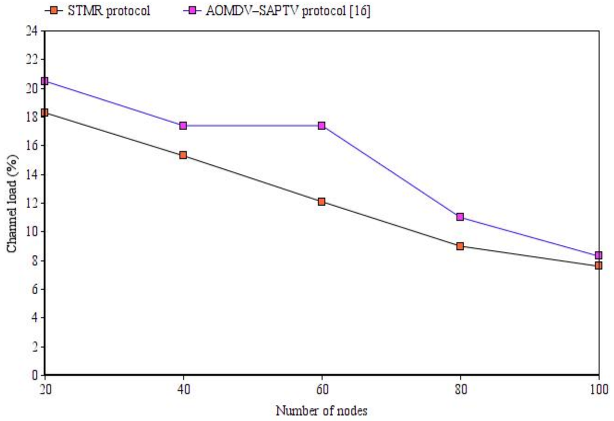
(b)



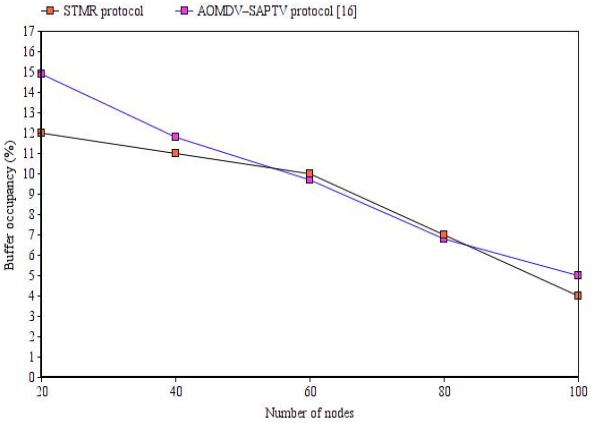
(c)



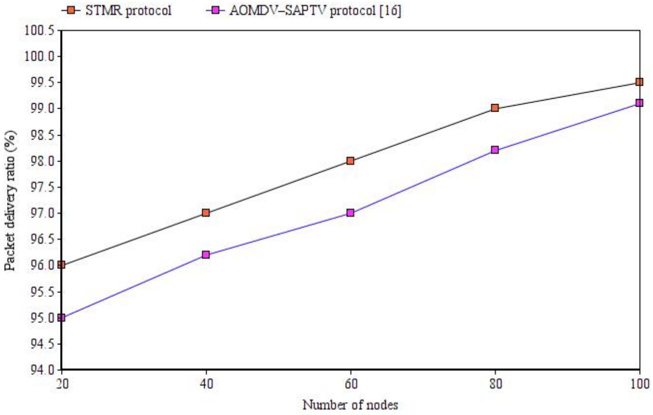
(d)



(e)



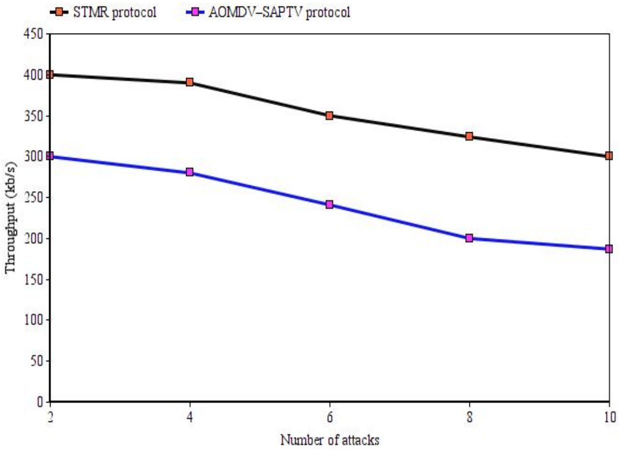
(f)



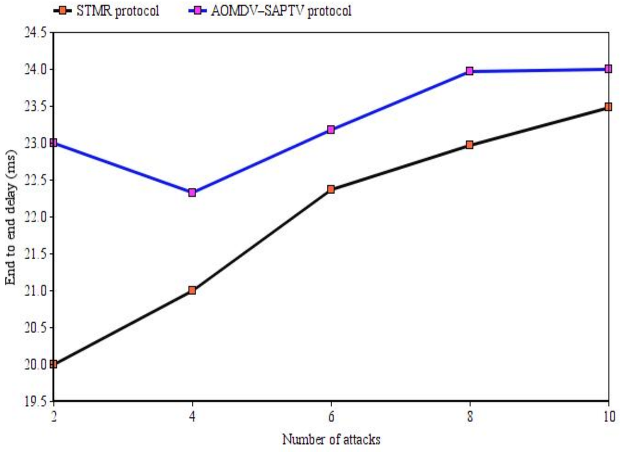
(g)

C. VARYING NUMBER OF ATTACKS

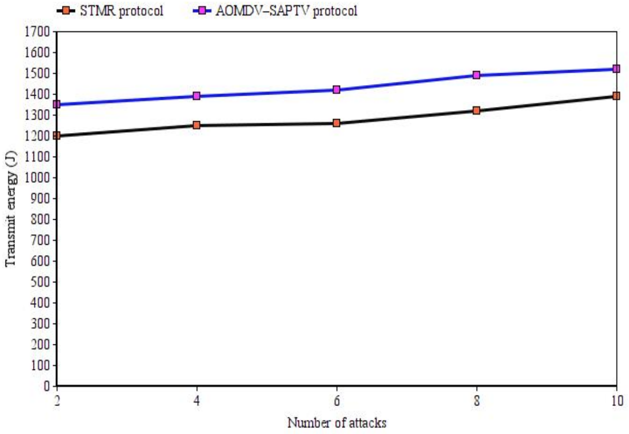
In this test, we vary the number of attacks as 2, 4, 6, 8 and 10, given in Table 2.The performance evaluation and the result comparison of proposed STMR and existing AOMDV–SAPTV protocol is given in Fig. 3a-g. The plots are clearly shows the results of different graph of proposed STMR protocol is very efficient than existing AOMDV–SAPTV protocol.



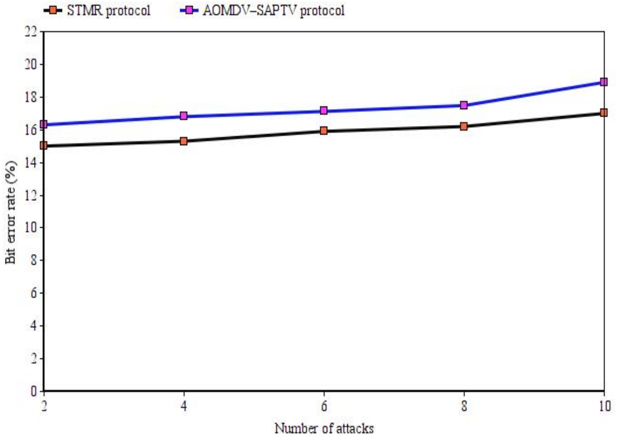
(a)



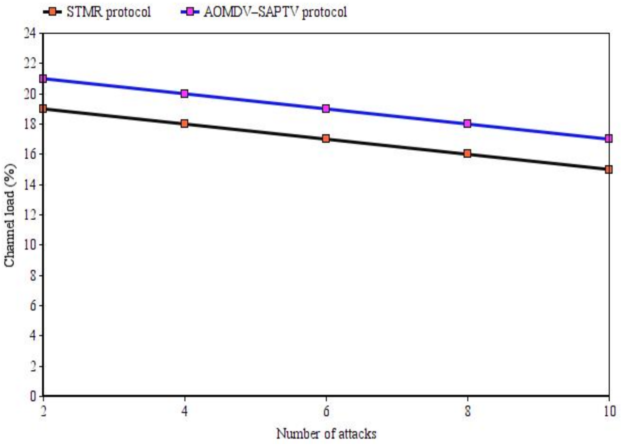
(b)



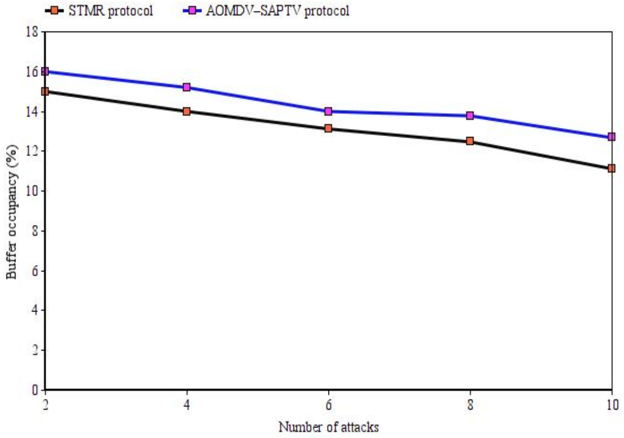
(c)



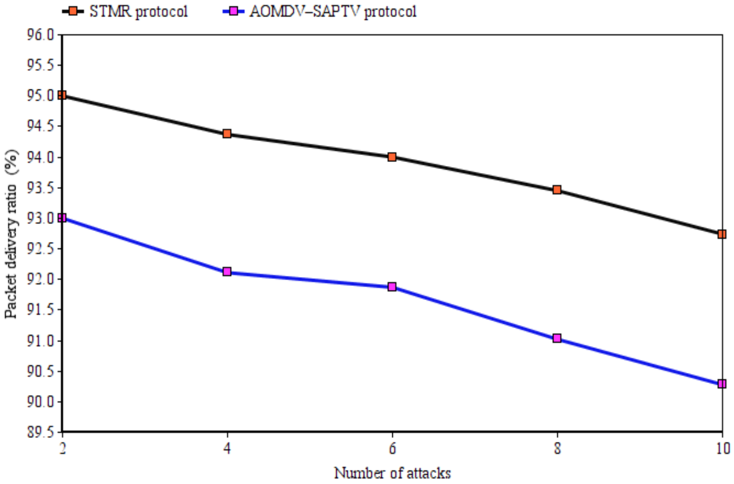
(d)



(e)



(f)



(g)

V1. CONCLUSSION

In this paper, we have proposed a secure token based multipath routing (STMR) protocol for MANET. The proposed STMR protocol consists of two processes are clustering and path selection. The proposed Triangle optimization algorithm is utilized to form the clustering and the multiple performance constraints used to compute the trust degree of each node. The highest trust degree is act as CH in the cluster among multiple mobile nodes. The multi-favor decision making algorithm is used to compute the optimal path among multiple paths. Finally, the proposed STMR protocol is applied to AOMDV to evaluate the performance. The simulation results proved that the effectiveness of proposed STMR protocol in terms of throughput, end to end delay, transmit energy, bit error ratecomparison, channel load, buffer occupancy and packet delivery ratio.

REFERENCES

1. Y. Cong, X. Zhou and R. Kennedy, "Interference Prediction in Mobile Ad Hoc Networks With a General Mobility Model", IEEE Transactions on Wireless Communications, vol. 14, no. 8, pp. 4277-4290, 2015.
2. A. Suneja, "Data Management and Synchronization in a Mobile Ad Hoc Network", IEEE Potentials, vol. 31, no. 2, pp. 28-30, 2012.
3. G. Di Crescenzo, R. Ge and G. Arce, "Securing reliable server pooling in MANET against byzantine adversaries", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 357-369, 2006.
4. Y. Liang, H. Poor and L. Ying, "Secrecy Throughput of MANETs Under Passive and Active Attacks", IEEE Transactions on Information Theory, vol. 57, no. 10, pp. 6692-6702, 2011.
5. S. Kumar and K. Dutta, "Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges", Security and Communication Networks, vol. 9, no. 14, pp. 2484-2556, 2016.
6. Y. Qin, D. Huang and B. Li, "STARS: A Statistical Traffic Pattern Discovery System for MANETs", IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 2, pp. 181-192, 2014.
7. W. Liu and M. Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585-4593, 2014.
8. Logeshwari, K., and L. Lakshmanan. "Authenticated anonymous secure on demand routing protocol in VANET (Vehicular adhoc network)." Information Communication and Embedded Systems (ICICES), 2017 International Conference on. IEEE, 2017.
9. Shawara, Mahmoud M., Amany M. Sarhan, and Nawal A. Elfishawy. "Energy aware Ad-Hoc On Demand Multipath Distance Vector (EA-AOMDV)." Computer Engineering Conference (ICENCO), 2017 13th International. IEEE, 2017.
10. Kamel, Mohammed Baqer M., Ibrahim Alameri, and Ameer N. Onaizah. "STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET." IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference. 2017.
11. Dhende, Sandeep, et al. "SAODV: Black hole and gray hole attack detection protocol in MANETs." Wireless Communications, Signal Processing and Networking (WiSPNET), 2017 International Conference on. IEEE, 2017.
12. Sridevi, N., and V. Nagarajan. "Enhanced secure wireless communication in MANETs." 2017 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2017.
13. Hmouda, Eljilani, and Wei Li. "Detection and Prevention of Attacks in MANETs by Improving the EAACK Protocol." SoutheastCon 2018. IEEE, 2018.
14. Joshi, Vaishnavi Bheemarao, and R. H. Goudar. "Intrusion detection systems in MANETs using hybrid techniques." Smart Technologies For Smart Nation (SmartTechCon), 2017 International Conference On. IEEE, 2017.
15. Naveena, Ambidi, and Katta Rama Linga Reddy. "Malicious node prevention and mitigation in MANETs using a hybrid security model." Information Security Journal: A Global Perspective 27.2 (2018): 92-101.
16. G. Borkar and A. Mahajan, "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", Wireless Networks, vol. 23, no. 8, pp. 2455-2472, 2016.

AUTHOR PROFILE

SJ Sultanuddin working as Assistent Professor in Department of Master of Computer , Measi Institute of Information Technology. A Research scholar in Sathyabama University. Completed MCA and Mtech., He has received 4 National conferences and 2 International conferences for his research contributions in International Journals of (Scopus & SCI). His area of Interest includes Wireless Networks, Mobie Ad hoc Networks and Web Security

Email : sayedjamalsultanuddin@gmail.com

Dr. Mohammed Ali Hussain working as Professor in Department of Electronics and Computer Engineering, KLEF Deemed to be University, Guntur Dist., Andhra Pradesh, India. He has received 5 National Awards and 2 International Awards for his research contributions in various International Journals (Scopus & SCI). He is Editorial Board Member & Reviewer of various International Journals. He has published 6 patents to his credit and produced 3 PhD’s under his supervision. His area of Interest includes Wireless Networks, Mobile Ad hoc Networks and Web Security.He is a member of various professional bodies FISEEE,ASDF, UACEE, IACSIT.

Email : alihussain.phd@gmail.com