International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 31565-31583

http://www.ripublication.com

Development Of Secure Cluster Based Multipath Routing Scheme For MANET

M. Kaliappan[1] and Dr.B.Paramasivan[2]

Assistant Professor (Senior Grade),
Dept of Information Technology, National Engineering College,
Kovilpatti, Tamil nadu,India[1].
Professor, Dept.of Computer Science and Engineering,
National Engineering College,
Kovilpatti, Tamil nadu,India[2]
kalsrajan@yahoo.co.in, bparamasivan@yahoo.co.co.in

ABSTRACT

Communication between mobile nodes is the most problematic issue for forwarding packets between mobile nodes in a MANET. Each node can forward data packets for other nodes using open media, which makes it possible for the malicious nodes to launch various attacks, such as a black hole attack, wormhole attack and rushing attack. It causes great security challenges and makes it difficult to design secure routing in a MANET. Secure routing plays a vital role in forwarding packets in critical applications. And also, the reliable routing of packets between the nodes becomes a very challenging in MANET because its dynamism of topology changes. Multipath routing is also a great challenge in MANET due to the dynamic network environment. Thus, Effective secure multi path routing and reliability are quite essential to protect nodes from anonymous behavior. In order to enhance the security and reduce the attacks, a secure cluster based multipath routing protocol (SCMRP) is proposed to establish multiple node disjoint routes and enhance security. A Hierarchical cluster formation technique is used to form the clusters. A cluster head is selected based on cluster weight factor that is considered as highest remaining energy, mobility factor and Transmission range. SCMRP create multiple paths between source and destination that eliminates unreliable routes. SCMRP also used Dynamic Secret based Encryption (DSE) to enhance security. During the routing establishment, dynamic encryption key is updated by the retransmission sequence. The simulation reveals that the SCMRP protects the nodes against eavesdropping by updating the dynamic encryption key with retransmission sequence in

routing even the attackers know the details of DSE scheme and obtain the encryption key at some time. SCMRP is simulated in network simulator 2 and compared with existing protocols. The simulation results shows that the proposed SCMRP outer performs than existing protocols.

Keywords: Black hole attack, Clustering, MANET, Multipath routing, Rushing attack, Wormhole attack.

1. INTRODUCTION

Mobile ad hoc networks (MANET) consist of more number of wireless mobile nodes and it is move freely and dynamically. MANET needs [16] the multiple hops to forward the packets due to its limited transmission range characteristics. And also, the reliable routing of packets between the nodes becomes a very challenging in MANET because its dynamism of topology changes. Multipath routing is also a great challenge in MANET due to the dynamic network environment.

A MANET is at a greater risk by allowing the extended presence of security attacks, but more likely to have preinstalled security mechanisms to detect these security attacks [1]. Malicious nodes in sparsely populated networks can be more harmful than malicious nodes in a densely populated network since these nodes can effectively not only disrupt communication but also disconnect the network. The level of effort required of resource constrained devices to monitor, detect, and diagnose malicious activity in a dynamic ad hoc network may be too costly when compared to the cost of simply rerouting packets through an alternative path. In a densely populated network where several alternative paths are typically available, selecting an alternative route may be a more judicious use of limited resources. A Diffie-Hellman key exchange protocol [24] is a suitable mechanism for obtaining secure communication in MANET. But sharing the keys between the source and destination is an issue owing to the unreliable communication offered in a critical environment. Further, to establish multiple node-disjoint routes in a route discovery attempt and exclude unreliable routes before transmitting packets, multipath routing scheme [22] is determined as a suitable mechanism for effective routing in MANET. This mechanism is followed in the proposed scheme for achieving energy efficient secure routing.

Existing secure routing protocols designed for a MANET face number of problems [5][23]. The problems include the fault detection mechanism is not considered into the network by data transmission strategy. It depends on the acquisition of network topology those points out the necessity of hiding topology in designing the routing protocols in MANET. To address these issues, it is desirable to design an efficient and secure cluster based multipath routing scheme for MANET. Further, designing secure multi path routing protocols require a detailed knowledge about technology followed in a MANET and their peculiar features relevant to security aspects. Thus, Effective secure multi path routing and reliability are quite essential to protect nodes from anonymous behavior. In order to enhance the security

and reduce the attacks, a secure cluster based multipath routing protocol (SCMRP) is proposed to establish multiple node disjoint routes and enhance security.

The SCMRP consists of three phases such as Cluster formation, Establishment of Multipath Routing and Secure path selection. A Hierarchical cluster formation technique is used to form the clusters. A cluster head is selected based on cluster weight factor that is considered as highest remaining energy, mobility factor and Transmission range. SCMRP create multiple paths between source and destination that eliminates unreliable routes. SCMRP also used Dynamic Secret based Encryption (DSE) to enhance security. During the routing establishment, dynamic encryption key is updated by the retransmission sequence. The simulation reveals that the SCMRP protects the nodes against eavesdropping by updating the dynamic encryption key with retransmission sequence in routing even the attackers know the details of DSE scheme and obtain the encryption key at some time.

The remainder of the paper organized five sections. Section 2 summarizes related work. Section 3 presents our proposed secure cluster based multipath routing protocol. Section 4 presents our simulation results and a relevant performance analysis. A section 5 presents our conclusions.

2. RELATED WORKS

Communication between mobile nodes is the most problematic issue for forwarding packets among mobile nodes in MANET. Each node can forward data packets for other nodes using open media which makes it possible for the malicious nodes to launch various attacks, such as black hole attack, wormhole attack and rushing attack. It causes great security challenges and makes it difficult to design secure routing in MANET. Yujun Zhang et al [5] proposed a TOpology-Hiding multipath Protocol (TOHIP) that analyzed the threats of topology exposure. It provides the capability to find better routes. TOHIP has more routing overhead than SRP when it is measured by bytes. And also in this paper, they did not use any efficient security algorithm to prevent the attacks. Ting Liu et al [2] applied the concept of dynamic secret to design an encryption scheme for smart grid wireless communication. It has good compatibility, which could be integrated with many wireless techniques and applications. Since the length of retransmission sequences are used to generate the secret key, the attackers can hack that secret key very easily.

Zhao et al. [3], proposed an Anonymous Location-based and Efficient Routing protocol (ALERT) in order to provide high anonymity protection (for sources, destination, and route) with low cost. ALERT is not completely bulletproof to all attacks. The delay of ALERT increases slightly in the group movement model. ALERT's random relay selection generates longer path length than the shortest path. Ranjeet et al. [4], addressed the issues and challenges of the various multipath routing protocols in MANETs. It ensures reliability, load balancing and QoS, multipath routing protocols have been proposed for MANET.They did not design a multipath routing protocol. They did not paid special attention to simultaneous usage of paths, data forwarding mechanism considering the delay of the available paths, scalability and energy efficiency. Gagandeep et al. [5], discussed various types of attacks on

various layers under protocol stack Different types of attacker attempts different approaches to decrease the network performance, throughput. They introduced different security mechanisms to prevent the dynamically changing environment. They did not invent such security algorithm, which will be installed along with routing protocols that helps to reduce the impact of different attacks. Zhao, et al. [10], proposed a risk aware response mechanism to systematically cope with routing attacks in MANET. A risk-aware response solution is used for mitigating MANET routing attacks. The mean latency of risk-aware response is higher than other response mechanisms when the network is smaller. Defrawy et al. [7], addressed a number of issues arising in suspicious location-based MANET settings by designing and analyzing a privacy-preserving and secure link-state based routing protocol (ALARM). The main advantage of the basic ALARM protocol is its simplicity and effectiveness. Since flooding is used to disseminate LAMs, scalability becomes problematic for large MANET. Any node can lie about its location or generate multiple LAMs as part of a Sybil attack. Zhang et al. [8] proposed a novel route discovery mechanism based on the estimated distance to reduce the control overhead of routing protocols in MANET. It is used to reduce the routing control overhead by restricting the propagation range of RREQ packets. The packet delivery ratio and the average end-to end delay give some negative effect when the node distribution is very sparse. Djahel et al.[9], designed a cross layer scheme that ensures higher detection accuracy. They have designed a cross layer scheme that ensures higher detection accuracy. If no shared node is identified then the source node delays or abandons the transmission of the data packets, leading to a severe degradation of the network performance.

Mohamed et al.[10]**,** present a protocol named as QoS and Load Balancing-AOMDV, a solution to achieve better load balancing with respect to the end-to-end QoS requirement. If one RREP is received, therefore only one route layout from source to destination is used to send data packets. If many RREP are received, the source chooses the best route based on the short number of "hop count". They did not calculate any routing parameters like distance, energy and link quality to select the best path**.** Y.B. Yang et al. [11], proposed a protocol which introduces a stability factor which conserves and stabilizes energy among the nodes, and a delay reduction mechanism which reduces the average end-to-end delay of the network. The protocol does not perform packet delivery ratio while maintaining the other quality of service parameters. Energy consumption of network can be reduced by decrementing the transmission power of the nodes depending on the minimum distance required for communication and energy level of node. Toh et al.[12], discussed the various load metrics and summarizes the principles behind several existing load balanced ad hoc routing protocols. This protocol does not perform load balancing during route discovery. Prayag et al. [13], proposed a method of message security using trust-based multi-path routing. They did not design a more efficient algorithm for selecting the routes from a set of routes.

Moreover, it almost turned the multipath routing scheme to increase network lifetime. Multipath Routing scheme reduces the routing overhead significantly. There are several schemes to find multiple loop-free paths in a route discovery, ad hoc on-

demand trusted-path distance vector (AOTDV) (Li et al 2010), enhanced multi-path dynamic source routing algorithm (EMP-DSR)[27], energy efficient secure multipath AODV[28], dynamic secret encryption scheme(DSEC)[6] are enhancing network lifetime. F.N. Abdesselam, et al. [14] devised an efficient method to detect and avoid wormhole attacks in the Optimized Link State Routing (OLSR) protocol. In OLSR each node periodically sends routing control messages, which increases the load in dense networks. As these routing control messages are tunnelled through the wormhole tunnel, the traffic increases dramatically, and congestion becomes inevitable through the path of that wormhole tunnel. This makes the legitimate nodes suspect and faultily identify some links as containing wormhole tunnels because of the increased delays. Papadimitratos et.al.[15], evaluated the secure message transmission (SMT) protocol and the secure single-path protocol for malicious disruption of data transmissions. SMT with link state allows us to isolate the performance of SMT from the underlying routing protocol and impose different limitations such as number of available routes, delays, and overhead. Secure Multipath Routing Protocol SMRP [23], proposed discovery algorithm with a security proof. This algorithm is vulnerable to a hidden channel attack. SMRP analyzed the security framework used for route discovery. An Authenticated Anonymous Secure Routing (AASR) [26] defends against potential active attacks without unveiling the node identities. In this scheme, the route request packets are authenticated by a group signature. AASR used a key-encrypted onion routing with a route secret verification message to prevent intermediate nodes from inferring a destination.

From the previous works, we had concluded that it is essential to design the multipath routing protocol. And also, it is necessary to select the best path for secure routing in MANET. TOHIP is not considered best path among multiple paths in MANET. AASR causes routing overhead by using more control packets to ensure the security. The proposed SCMRP detect a best path among multiple paths by considering energy, link quality and minimum distance between nodes. However, this scheme is unable to address secure routing effectively, selective dropping attack and energy consumption caused by a number of attackers in a MANET. It is essential to design the multipath routing protocol. And also, it is necessary to select the best path for secure routing in MANET. The best of our knowledge, it is a first work to enhance the security in multipath routing.

3. PROPOSED SECURE CLUSTER BASED MULTIPATH ROUTING SCHEME

The proposed scheme purposely observed the issues of secure cluster based multipath routing in MANET which allows the multiple paths between a source and destination. The proposed scheme used a Dynamic Secret based Encryption scheme in multipath that provide the security during the transmission of packets. And also, it is very important to select a path with no malicious node from the multiple paths to achieve secure routing. The better path is selected by considering the metrics such as energy, distance and link quality. The proposed method consists of following phases

- Cluster formation

- Establishment of Multipath Routing
- Secure path selection

1.1 CLUSTER FORMATION

The SCMRP used a Hierarchical based cluster formation technique to partition the group over a variety of scales. It used a methodology for selecting energy efficient cluster head. A cluster weight factor is calculated for the mobile node based on the metrics such as highest remaining energy, mobility factor and Transmission range. The highest remaining energy of all nodes is calculated by Equation(1)

$$E_{HR} = E_T - (E_I + E_{Tx} + E_{Rx}) \quad (1)$$

Where E_{HR} is the highest remaining energy, E_T is the total energy, E_I is the initial Energy of node, E_{Tx} is the transmission energy, and E_{Rx} is the receiving energy. The mobility of node is calculated as the rate of position of mobile node with respect to time. Nodes update packets frequently at high speed during travel. Here, node with less mobility is considered as factor. Source node knows the mobility of all nodes. Mobility of a node is expressed by Equation(2)

$$M_f = \frac{1}{T} \sum^{T} \sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2} \quad (2)$$

M_f- mobility of a node $\sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2}$ is the distance between sender and all nodes. T is the time. During the route request phase, the sender node calculates the distance between sources nearest nodes. Transmission range is calculated by Equation (3)

$$TR = \prod * \sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2} \quad (3)$$

A node with highest weighted factor is selected as a cluster head that is based on a weighted factor such as the highest remaining energy, the less mobility and the large transmission range. The aim of clustering process is eliminate far away nodes to participate in the routing process. The Figure 6.1 shows the scenario of secure cluster based multipath routing in a MANET. In this scenario, nodes 4, 8, 9 and 21 are not involved in the routing phase. This process also increases the network lifetime.

1.2 ESTABLISHMENT OF MULTIPATH ROUTING

This section presents the establishment of multipath routing in MANET. Multipath routing possesses three phases: route request phase, route reply phase and route probe phase.

- Route request phase creates a reverse route which is used in route reply phase. In this phase, route request messages are transmitted from source to destination. After receiving the route request message, every intermediate

node creates a reverse route and rebroadcast them if the message is not received before.

- Route reply phase finds many node disjoint routes as possible in route message. In this phase, route reply messages are transmitted from destination to source node. After receiving a reply message, an intermediate node picks the neighbor which is close as to the source node and therefore multiple node disjoint routes are established.
- Route probe phase detects the unreliable route and exclude it before send out the packets. The source node sends a route probe message through every exposed route in route reply message to the destination node. By performing this action, the unreliable route is detected and eliminated.

In these three phases, every node maintains two tables. One is Sequence Number Table (SNT) which is used to prevent nodes from unnecessary route messages. The other is a Routing Table (RT) that includes the node through which to reach the destination and determine the number of hops to the destination.

1.3 SECURE PATH SELECTION

A best path is selected from the multipath by considering the matrices such as energy, link quality, and distance. The shortest distance of a routing path is calculated by Equation (4)

$$d_{min} = \sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2} \quad (4)$$

The Energy of a route is calculated by Equation (1). The link quality between nodes is measured by radio signal strength that found by Equation (5)

$$l_q = \frac{s_p}{s_{max}} \quad (5)$$

Where, S_p is the signal strength and S_{max} is the maximum strength available. Finally, a path with minimum distance, efficient link quality and maximum energy is selected as a better path for transmission. Security mechanism is applied in the selected path for enhancing secure data transmission. It detects three security attacks such as wormhole attack, black hole attack and rushing attack during the communications between the nodes in a selected path.

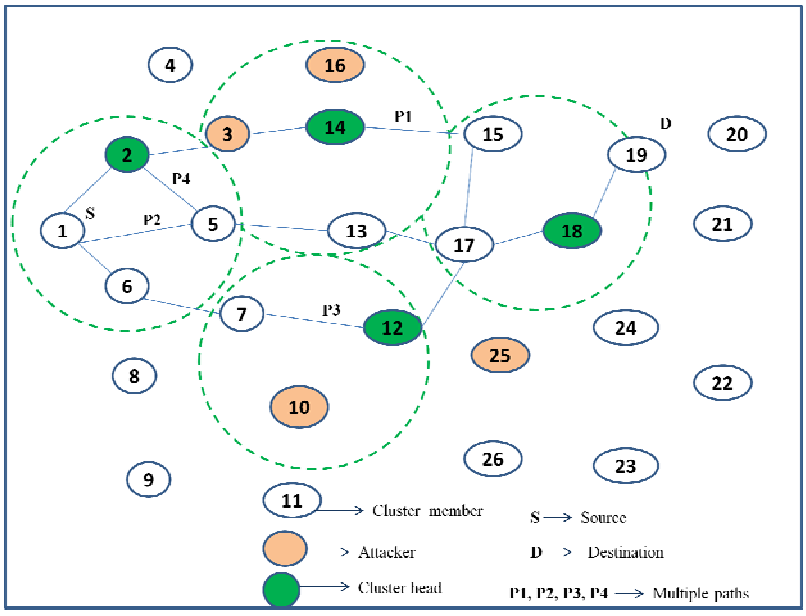

Figure 1: Scenario for secure multipath routing

Figure 1 shows the secure multipath routing scenario. Initially, the source(S) initiates Route Probe Phase (RPRO) by sending a route probe message to the destination (D) through every route that has been established in Route Reply Phase. In every RPRO, D is required to send a RPRO message back to S through a reverse route. In RPRO phase, S detects the secure routes. If there are malicious nodes present in the path p1 that may drop the packets. S may not receive the returning RPRO message on that path p1. Immediately, S selects another path like p4 or p2 according to figure6.1.

In wormhole attack, an attacker records packets or bits at one location in the network, tunnels them to the selected location, and retransmits them into the network. Wormhole nudes fake a route that is shorter than the original one within the network; this can confuse the routing mechanism which relies on the knowledge about the distance between nodes. The attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally. The tunnel is either wired link or a high frequency links. This creates the false impression that the two end points of the tunnel are very close to each other which leads to routing disruption. In a MANET, a black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. Black holes refer to places in the network where incoming or outgoing traffic is silently discarded without informing the source that the data did not reach its planned receiver. When investigating the topology of the network, the black holes themselves are hidden, and can only be identified by observing the lost traffic.

When a node sends a route request packet (RR) to another node in the network, if there an attacker present, then it accepts the RR packet and sends it to their neighbors with higher transmission speed as compared to other nodes. Because of this

high transmission speed, packet forwarded by the attacker first reaches to the destination node. Destination node accepts this RR packet, and discards other RR packets which are reached later. Receiver found this route as a valid route and use for further communication. This way attacker successfully gains access in the communication between sender and receiver.

In order to prevent attacks, the proposed scheme used a Dynamic Secret based Encryption Scheme (DSE). DSE is applied in a selected path to enhance the security and reduce the attacks during communication. A dynamic secret concept is applied to design an encryption scheme for node communication. Between two nodes of communication, the previous packets are coded as retransmission sequence, where the retransmitted packet is marked as ′1′ and the other is marked as ′0′. During the communication, the retransmission sequence is generated on both sides to update the dynamic encryption key. Any missing in retransmission sequence would prevent the adversary from achieving the keys. Considering the limitation on computational power, the hash functions are used in the Dynamic secret generation that is expressed by Equation (6.6)

$$ds(k) = f_1 H(\varphi_1(L_1 Rs)) \tag{6.6}$$

where ds(k) is the dynamic secret key, f1H is the hash function, and Rs is the re-transmission sequence. The new dynamic secret is applied to update the dynamic encryption key (DEK) that is calculated by Equation (6.7)

$$\text{DEK (k)} = \text{Ds (k)} \oplus \text{DEK (k-1)} \tag{6.7}$$

A DEK is generated on both sides of communication synchronously. The sender applies it to encrypt the, and the receiver applies it to decrypt the. XOR function is applied to update the DEK that is used for encrypt or decrypt the data on both sides. Encryption and decryption are expressed as follows.

$$D \oplus Dek^{*}(k) = C_D \tag{6.8}$$

$$C_D \oplus Dek^{*}(k) = D \tag{6.9}$$

If DEK is shorter than the data, is replicated and padded circularly to generate whose length is equal to the raw data or cipher text. DSE scheme is an appropriate solution for securing wireless communication. It can prevent eavesdropping and forging by utilizing the inevitable errors in communication

4. RESULTS AND DISCUSSION

4.1 Simulation study

The proposed scheme has been implemented in network simulator (NS2). The main objective of the simulation was to enhance energy efficiency to increase the network

lifetime. 100 nodes were randomly deployed in a 1000 m x 1000 m area of interest. The transmission range of the node was 50 m and initial energy is assigned with 10 joules. Nodes followed the random waypoint model that finds the availability of connection paths in MANET, where nodes are moving at six different uniform speeds ranging between 0 to 30 m/s. The proposed schemes also evaluated by comparing it with the related TOHIP, AASR and SMRP protocols in terms of the packet delivery ratio, energy consumption, throughput and routing overhead. The simulation results were studied by varying the network size from 50 to 200. Table 1 shows the simulation parameter setting for the evaluation of a proposed scheme and the related schemes.

Table 1 Simulation parameters

Parameter	value
Simulation area	1000m x 1000m
Number of mobile nodes	50,100,150,200
Simulation time	500sec
Number of source–destination pair	10
Node movement speed	30 m/sec
Initial energy	10 j
Transmit energy	0.5j
Receiver energy	0.1j
Ideal energy	0.01j
Packet size	512 bytes
Number of attacker	20

4.2 Results and discussion

This section describes the results obtained through simulation of the proposed scheme. The experimentation is performed by varying the count of attackers in the network. The results obtained are analyzed by varying the size of the network. The efficiency of the proposed and related schemes is evaluated using the metrics such as, Packet delivery ratio, total energy consumption, end-to-end delay, signal strength ratio, and routing overhead. The simulation results show that the proposed scheme achieves maximum efficiency when compared with other related schemes.

Packet delivery ratio: The packet delivery ratio can be determined as the ratio of the number of packets successfully delivered to the destination of the number of packets sent by the source along the path. It shows the capability of the proposed mechanism to deliver the data to the destination.

End to end delay: The end to end delay refers to the time taken for a packet to be transmitted across a network from source to destination

Routing overhead: refers to the total number of routing packets are transmitted during the simulation time from source to destination. For packets sent over multiple hops, each transmission of the packet counts as one transmission. The proposed scheme has been estimated the routing overhead in varying nodes.

Total Energy consumption: Total energy consumption is total energy that is spent to deliver the packets successfully across a network from source to destination.
Signal strength ratio: The Signal Strength Ratio displays the ratio of the Vertical path received signal power to the Horizontal path received signal power. This ratio can be useful for determining multipath conditions in ad hoc networks.

4.2.1 End to end delay

The figure 2 shows that the proposed schemes SCMRP achievable minimum delay about 0.6sec for forwarding packets to the destination in the presence of 20 attackers, because the proposed scheme selected the energy efficient, secure attacker free routing path to involve the packet transmission. It also chosen alternate path for forwarding packet when the attacker present. It shows that the SCMRP achieved minimum delay compared to related schemes because it is not considered attacker to involve in the routing phase. The proposed scheme and related schemes TOHIP, SMRP and AASR have the end-to-end delay in the range of 0.6sec, 0.7sec, 0.79sec and 0.8sec respectively in the presence of attacker. The figure 3 shows that this metric keeps relative stable, which proves that the proposed SCMRP does not degrade the efficiency of delivering packets with minimum delay at maximum speed 30 m/sec. It also provides the secure multipath routing with the best path when compared to the existing methods.

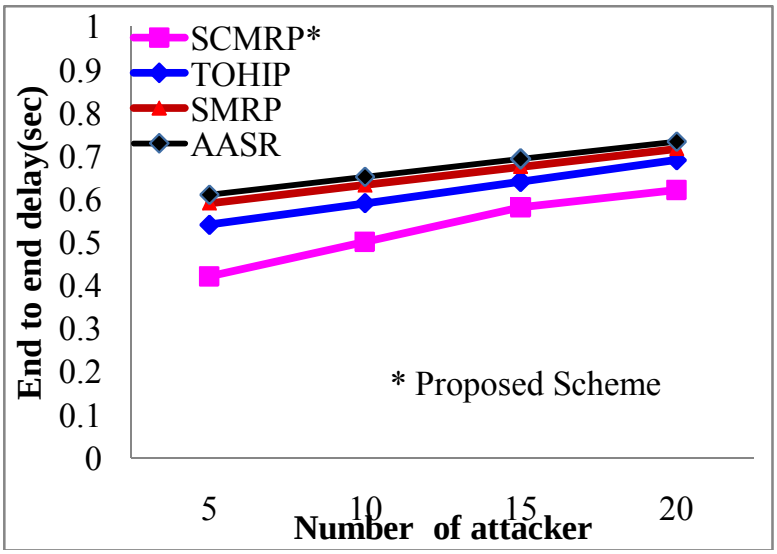

Figure 2:End to end delay vs. no of attacker

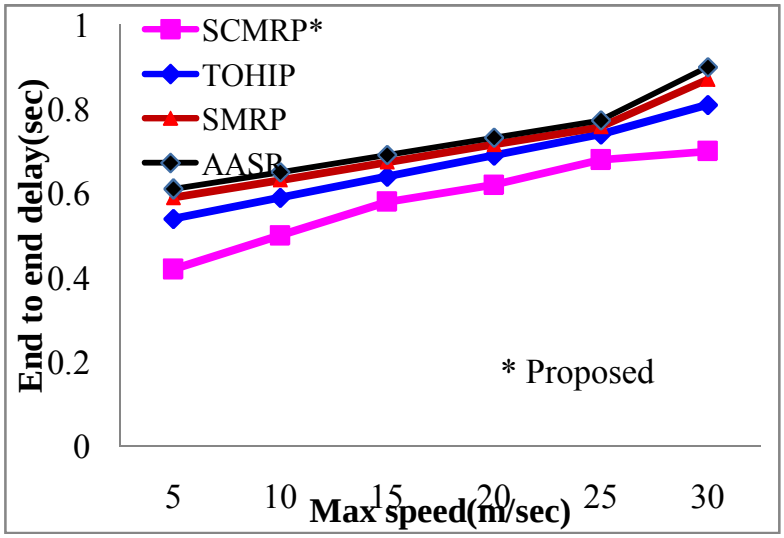

Figure 3: End to end delay vs. speed

4.2.2 Routing overhead

The figure 4 shows the evaluation of routing overhead for SCMRP, TOHIP, AASR and SMRP while varying the number of nodes. It is defined as number of routing packets transmitted for establishing routing paths that caused minimum routing overhead. Figure.4 clearly shows that the routing overhead caused by SCMRP has transmitted less routing packets than related schemes. SCMRP has transmitted average of 4500 routing packets for forwarding packets in the selected routing path with scheduled simulation time. The related schemes had required more routing packets for routing purpose that led routing overhead.

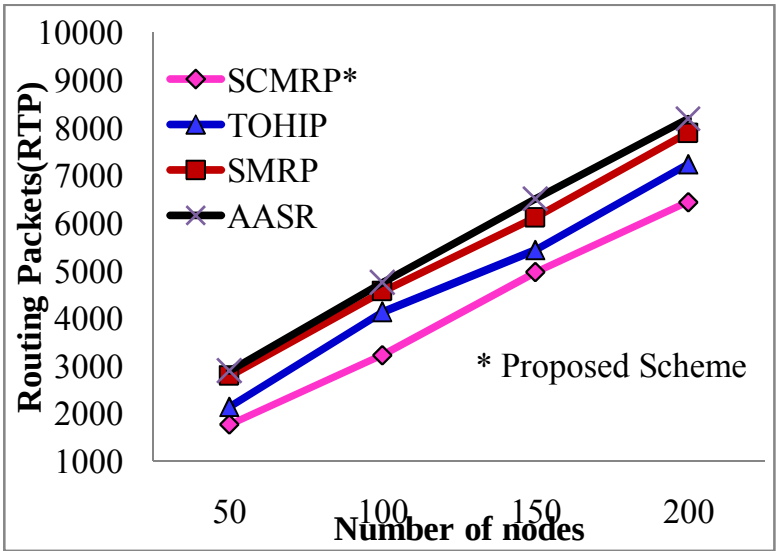

Figure 4: Routing overhead

4.2.3 Packet delivery ratio

The figure.5 shows the packet delivery ratio (PDR) by varying the nodes in the network. The SCMRP scheme compared with related schemes TOHIP, SMRP and AASR. It shows that the proposed schemes are maintained higher PDR about 97%. An intensive performance evaluation shows that the proposed has better capability of finding routes. When there are malicious nodes, the proposed can greatly improve the packet delivery ratio. The PDR of proposed schemes get increased when the number of nodes increases. It shows that the packet delivery ratio increases for the proposed model since it provides the multipath routing with the secure path when compared to the existing methods. It was shown that the performance of the proposed scheme is more efficient than the related schemes. Normally the value of PDR gets increased in the proposed model since it sends the number of data in a time when compared to the related schemes. It has been shown that the value of PDR increases since it provides secure multipath routing with the best path.

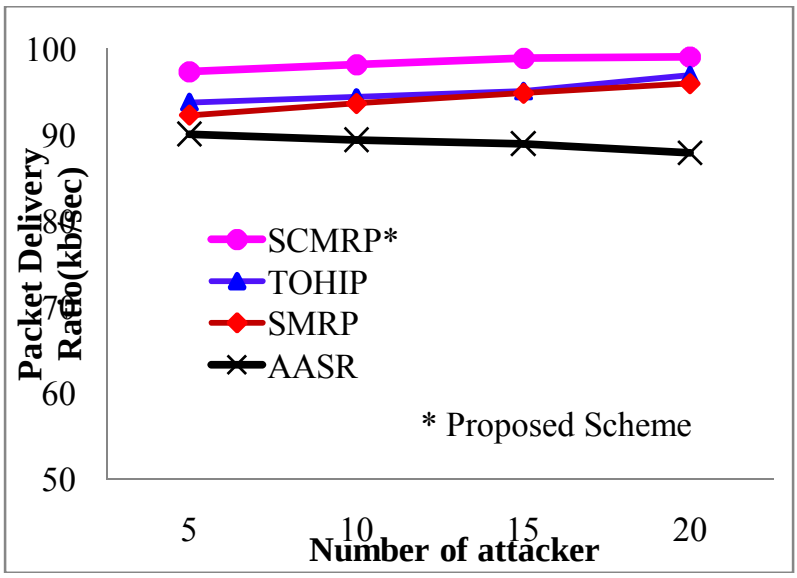

Figure5: Packet delivery ratio

4.2.4 Energy consumption of a network

The **f**igure 6 shows that the average energy consumption of a network in the network while varying number of nodes. It is noticed that the SCMRP consume minimum energy about 20 j while varying number of nodes. TOHIP has longer convergent time because it tends to establish longer routes and to find as many node-disjoint routes as possible in a route discovery attempt to prevent route discovery from being invoked frequently. The other twp related schemes such as SMRP and AASR does not considered energy factor and also it required more control packets to establish secure routing that causes consume more energy. The proposed SCMRP selects a best shortest path that offers more efficient results in less energy consumption. In proposed SCMRP, the energy consumption of a node increases slightly as the number of nodes increases. This is because the clustering technique provides minimum node to

participate in the routing. Also this figure shows that SCMRP does not consume more energy. It shows that the average energy consumption of nodes slightly increases within the acceptable range about 20j.

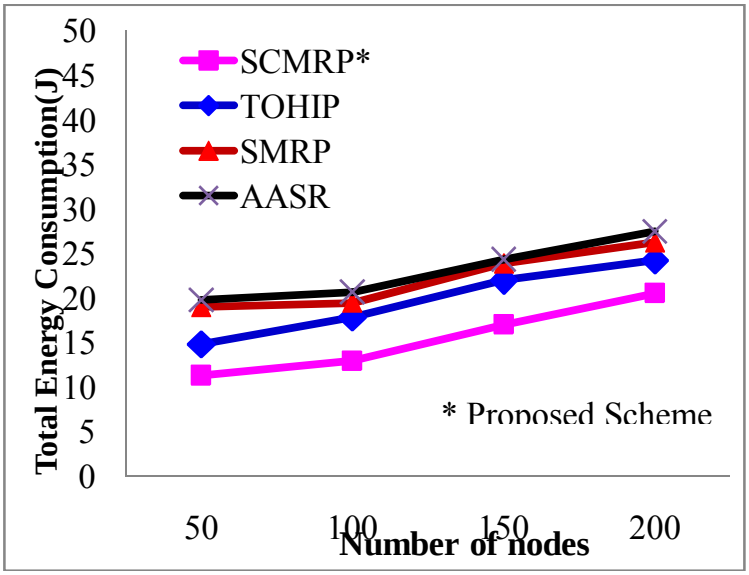

Figure 6: Energy consumption of network

4.2.5 Signal strength ratio

The figure.7 shows the signal strength ratio (SSR) by varying the nodes in the network. It shows that the proposed schemes are maintained more SSI than related schemes. The SSR of SCMRP gets increased when the number of nodes increases. It shows that the packet delivery ratio increases for the proposed model since it provides the more link quality between nodes in selected best path that shows a more efficient for forwarding packets without loss. The related schemes have less SSI because it was not considered link quality for establishing routing paths. Normally, the value of SSI gets increased in the proposed scheme. Since, it sends the number of data in a time when compared to the related schemes.

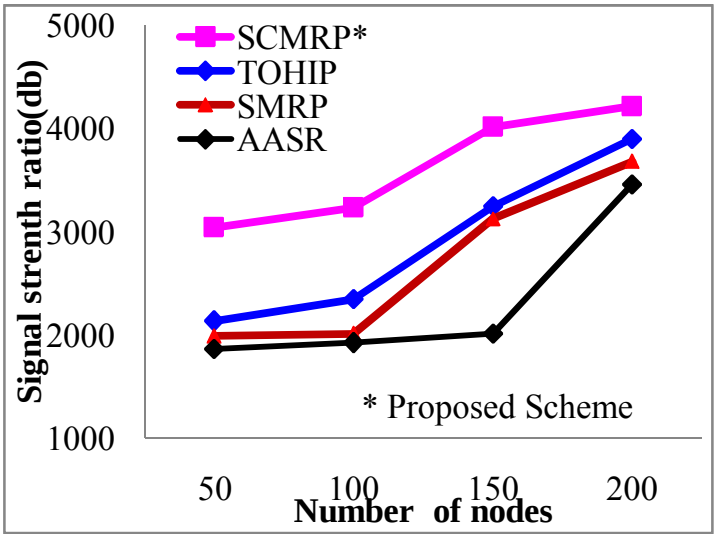

Figure 7: Signal strength ratio

Table 2 Comparative analysis of SCMRP with existing schemes.

Performance Metrics	**TOHIP**	**SMRP**	**AASR**	**SCMRP Proposed**
End-to-End delay(sec) vs. no of attacker	0.7	0.79	0.8	0.6
End-to-End delay(sec) vs. maximum speed	0.81	0.87	0.9	0.7
Total energy consumption(j)	24.23	26.22	27.45	20.52
Packet delivery ratio(kb/sec)	96.94	95.98	87.91	99.07
Signal strength Ratio(db)	3897	3678	3456	4213
Routing Overhead (RTP)	7235	7899	8189	64440

Table 2 shows the comparison of SCMRP with the related schemes for different parameters. The parameters may be the End-to-End delay, packet delivery ratio, routing overhead, energy consumption and signal strength ratio. The proposed scheme achieved less energy consumption, delay and routing overhead because it forms stable clusters with multipath in a network. The proposed scheme achieved higher PDR through secure data transmission because it selects a best path with which provides malicious free routing. The proposed scheme based network shows stability with increasing number of nodes in terms of energy consumption. The proposed scheme makes use of dynamic encryption scheme to achieved secure packet transmission. In existing schemes, the entire data can be exposed to the attacker during data transmission. The proposed scheme resists the attacker activities in routing by chosen alternate path for data transmission and is capable of achieving high packet delivery ratio with increased network lifetime.

5. CONCLUSION

The proposed secure cluster based multipath routing scheme establish secure route to increase the reliability and enhancing security of the network. The objective of the proposed SCMRP is to minimize the security risk caused by a attacker present in a network. The SCMRP consists of three phases such as Cluster formation, Establishment of Multipath Routing and Secure path selection. The energy efficient clusters are formed using a hierarchical clustering technique. The cluster weight factor such as highest remaining energy, mobility factor and Transmission range are considered to select a cluster head. The SCMRP also formed the multiple paths between source and destination and also it eliminates unreliable routes. Then, the best path was selected from the multipath by considering the parameters like energy, distance, link quality. A security mechanism DSE is applied in a selected path to enhance the security and reduce the attacks during communication. Finally, the performance of the network is evaluated when there is an attacker present in the network.

The major benefits of proposed scheme are i) secure routing path is established for the data transmission ii) if a attacker is found in a path, alternate path can be selected from the available multiple paths which provides efficient packet delivery ration. iii) The computation and routing overhead involved for security mechanism is very low compared to other related schemes. The achievability of the proposed scheme is evaluated through performance analysis and simulation results. The results show that proposed scheme outperforms well compared to the existing schemes in terms of packet delivery ratio, signal strength ratio, routing overhead, end to end delay and energy efficiency. Hence, proposed scheme can achieve high reliability and enhanced security in a vulnerable environment. This scheme is suitable for sensitive data transmission application.

REFERENCES

[1] Aarti & S. S. Tyagi 2013, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, vol.3,no.5, pp.252-257

[2] Priyanka Goyal, Vinti Parmar & Rahul Rishi 2011, "MANET: Vulnerabilities, Challenges, Attacks, Applications", IJCEM International Journal of Computational Engineering & Management, vol.11, pp.32-37.

[3] Mohit Kumar & Rashmi Mishra 2012, "An Overview of MANET: History, Challenges and Applications", Indian Journal of Computer Science and Engineering (IJCSE), vol.3, no.1.

[4] Stephen Mueller , Rosep. Tsang &Dipak Ghosal 2004, "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges", University of Calfornia , vol.2965, pp.209-213.

[5] Yujun Zhang, Tan Yan,Jie Tian, Qi Hu, Guiling Wang & Zhong cheng Li 2014," TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks", Journal of Ad hoc networks, vol.21, pp.109-122.

[6] Ting, L , Yang, L , Yashan, M , Yao, S , Xiaohong, G , Weibo, G & Sheng, X 2014, "A Dynamic Secret Based Encryption Scheme for Smart Grid Wireless Communication", IEEE Transactions on smart grid, Vol.5, no.3, pp.1175–1182.

[7] L.Y. Zhao & H.Y. Shen 2013, "ALERT: an anonymous location-based efficient routing protocol in MANETs", in Proceedings of *International* Conference on Parallel Processing (ICPP), pp.703-712.

[8] Ranjeet Kaur , Rajiv Mahajan & Amanpreet Singh 2013, "A survey on multipath routing protocols for MANETs", International Journal of Emerging Trends & Technology in Computer Science, Vol.2, no.2, pp.42-45.

[9] Gagandeep, Aashima & Pawan Kumar 2012, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), vol.1,no.5,pp.269-275.

[10] Ziming Zhao , Hongxin Hu , Gail-Joon Ahn & Ruoyu Wu 2011, "Risk-Aware Mitigation for MANET Routing Attacks", IEEE Transactions on Dependable and Secure Computing, Vol.9, no.2, pp.250 - 260.

[11] K.E. Defrawy, G. Tsudik 2014, "ALARM: anonymous location-aided routing in suspicious MANETs", IEEE Transactions on Mobile Computing, vol.10,no.9, pp.1345_1358.

[12] Xin Ming Zhang , En Bo Wang , Jing Jing Xia & Dan Keun Sung 2011, An Estimated Distance-Based Routing Protocol for Mobile adhoc networks, IEEE Transactions on Vehicular Technology, Vol.60, no.7, pp.3473 - 3484.

[13] Djahel, S , Nait-abdesselam, F & Zonghua Zhang 2011, Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges, IEEE Communication Survey & Tutorials, Vol.13, no.4, pp.658-672.

[14] Mohamed Tekaya , Nabil Tabbane & Sami Tabbane 2010, Multipath Routing with Load Balancing and QoS in Ad hoc Network, International Journal of Computer Science and Network Security, Vol.10, no.8, pp.280-286.

[15] Y.B. Yang, H.B. Chen, An improved AODV routing protocol for MANETs", in proceeding of International Conference on Wireless Communications, Networking and Mobile Computing (WiCom), 2009, 1_4.

[16] Chai Keong Toh , Anh-Ngoc Le & You-Ze Cho 2009, Load balanced routing protocols for ad hoc mobile wireless networks, IEEE Communications Magazin, Vol.47, no.8, pp.78 - 84.

[17] Prayag N , Sanjay Kumar , D , Sudip Misra & Isaac, W 2008, Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing, Computer Communications, Vol.31, no.4, pp.760-769.

[18] Nait-Abdesselam, F , Bensaou, B & Taleb, T 2008, Detecting and avoiding wormhole attacks in wireless ad hoc networks, IEEE Communications Magazine, Vol.46, no.4, pp.127 - 133.

[19] Papadimitratos, P & Haas, ZJ 2006, Secure data communication in mobile ad hoc networks IEEE Journal on Selected Areas in Communications, Vol.24, no.2, pp.343 - 356.

[20] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay 2010, "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS), vol.4, no.3, pp.265-274.

[21] Satyam Shrivastava 2013, "Rushing Attack and its Prevention Techniques", International journal of Application or Innovation in Engineering and Management, vol.2, no.4

[22] Abbas, AM & Jain BN 2010, Path diminution in node-disjoint multipath routing for mobile ad hoc networks is unavoidable with single route discovery, Journal of Ad Hoc and Ubiquitous Computing, Vol.5, no.1, pp.7-21.

[23] Burmester, M & Medeiros, B 2009, "On the security of route discovery MANETs", IEEE Transaction on Mobile Computing, Vol.8, no.9, pp.1180–1188.

[24] Shobana, M & Suresh, S 2013, "Secure Clustering and Energy Based Routing for Mobile Adhoc Networks", Emerging Technology and Advanced Engineering, Vol.3, no.3, pp.728-734.

[25] Li, Y & Wang, P 2010, "Cluster cache based k-hop clustered routing protocol", Proceedings of 6th International Conference on Wireless Communication Networking and Mobile Computing(WiCOM), , pp.1–4.

[26] Wei Liu & Ming Yu 2014, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments" , IEEE Transactions on Vehicular Technology, Vol.63, no.9, pp.4585 - 4593.

[27] Asl, EK , Damanafshan, M , Abbaspour, M , Noorhosseini, M & Shekoufandeh, K 2009, "EMP-DSR: An Enhanced Multi-path Dynamic Source Routing Algorithm for MANETs Based on Ant Colony Optimization", Proceeding of Modelling & Simulation , pp.692 - 697.

[28] Jain, HR & Sharma, SK 2014, "Improved energy efficient secure multipath AODV routing protocol for MANET", Proceeding of International Conference on Advances in Engineering and Technology Research , pp.1-9.

BIOGRAPHY

M.Kaliappan born in Srivilliputtur,Tamil nadu, India, on March 26, 1977,received his B.E. degrees in Computer Science from Madurai Kamaraj University, Tamilnadu,India in 1999 and M.E degree in Computer science and Engineering from Ma-non manian Sundaranar University ,Tamilnadu , India in 2011. He is currently an Assistant Professor(Senior Grade) in National Engineering College ,kovilpatti, Tamilnadu . Now he has published two papers in International Journals and Four Papers in International Conferences. His main research interests include Security in Adhoc Net-works and cloud computing.

Dr.B.Paramasivan is 46 years old.He completed B.E degree in Computer Science and Engineering under Madurai Kamaraj University,Tamil nadu,India. He obtained M.E degree in Computer Science and Engineering under Jadavpur University ,Kolkatta, India. He received Ph.D degree from Anna University ,Chennai,India in the area of Wireless Sensor Networks. He is working as a Professor and Head in Department of Computer Science and Engineering,National Engineering College, Kovilpatti,Tamil nadu,India. He has published more than fifteen papers in National and International Journals. He has also presented more than thirty papers in various National and International Conferences. He has organized more than ten seminars sponsored by various Government funding agencies.He is an active member of various professional bodies like IE and CSI. His research interests include Wireless Adhoc and Sensor Networks ans high-performance networking