SURVIVAL STUDY ON ATTACK DETECTION AND ISOLATION TECHNIQUES FOR MULTIPATH AND MULTICAST ROUTING IN MANET

A.S.NARMADHA , DR.S.MAHESWARI , DR.J.NANDHINI , G.KALAIARASI

Abstract — A Mobile Ad hoc NETwork (MANETs) is a collection of wireless mobile nodes whereexchange of data packets arecarried out by not depending ona fixed base station or a wired backbone network. Routing is the process of transferringdata packets from a source to a destination in an inter-network. The routing process helps in forwarding the data packetswith help of routing tables that preserve a record of routes to many network destinations.Multipath routing selects more than one path between the source and destination nodes for packet transmission.Multicast routing sends the data packets to multiple receiver at a same time with minimal data traffic. But, MANET is more vulnerable to security attacks during the multipath and multicast routing which reduces the communication security level.In order to improvethe communication security in MANET, the attacks are to be detected and isolated during routing process. Our research work is concentrated on different attack detection and isolation for attaining improved communication security during routing process in MANET.

Keywords — Mobile Ad hoc Network , routing , Multipath , Multicast , Communication security , Attack detection , Isolation.

I. INTRODUCTION

MANET is a group of self-governing and self configurable nodes gets linked with help of wireless links and move randomly at any direction. MANET is mainly used in military and emergency operations as it provide an immediate network configuration without anyfixed infrastructure. Each node performsas terminal and router. It helps in transmitting the data packets to nodes that are not in transmission range of source node. Routing protocol denotes the communication policy in which the mobile nodes are more helpful in broad casting the information.

Multipath routing is the process of forwarding the data packets from source node to destination node through multiple paths. When multipath routing protocols are used, the path failures and the delay induced with path disconnection are reduced. Multicast routing is an essential one where the data is delivered from one source to many destinations at the same time. Multicasting reduces the data traffic as it requires the transmission of one packet by source and reuses the packet when required. MANET is vulnerable to security attacks because of the lack of a trusted centralized authority. Security in MANET is a key concern for secure communication between the mobile nodes in hostile environment.

This paper is structured as follows: Section II reviews on existing attack detection and isolation technique during multicast and multipath routing in MANET, Section III gives brief discussion about attack detection and isolation technique, Section IV identifies the possible comparison between them, Section V explains the limitations as well as the related work and Section VI concludes the paper, key areas of research is given as toimprove the attack detection rate and security level during multicast and multipath routing in MANET.

II. LITERATURE REVIEW

A MANETis established without any centralized and dedicated servers. The solution given is to preserve the networkagainst the blackhole attack.An efficient defense technique is introduced in [1] to fight against blackhole attack for identifying the secure routethroughimproving the performance of packet processing technique in normalAODV with minimal routing overhead and delay. However, the attack detection rate is not enhanced. A newnode authentication method is designed in [2] for authentication purpose when new node joined into network before starting the route discovery process in MANET.But, the performance of throughput, delay and packet delivery ratio is ineffective during the routing in MANET.

A distributed cross-layerbased machine learning anomaly detection system is implemented in [3]

A.S.Narmadha , Assistant Professor / ECE , Jayshriram Engineering College , Tirupur .

Dr.S.Maheswari , Assistant Professor (Sr.Gr) , Kongu Engineering College , Erode .

Dr.J.Nandhini , Assistant Senior Professor / ECE , Jayshriram Engineering College , Tirupur .

G.Kalaiarasi , Assistant Professor / ECE , Jayshriram Engineering College , Tirupur .

formulticast communication in MANET. The accuracy of Intrusion Detection System(IDS) increases the detection of direct and indirect internalstealthy attacks. However, the black hole and stealthy attack is detected and isolated using cross-layer based machine learning anomaly detection system. A security solution termedHoneypot-Based Dynamic Anomaly Detection by Cross-layer Security (HBDADCS) is introduced in [4] is carried out for blackhole.

An auto configuration scheme in [5] addresses the security problems. The protocol uses the grid based hierarchical architecture for solving the duplication detection issues. However, the processing time remains sameas it performs authentication and hashing process.An algorithm introduced in [6]is to identify existence of the SYN flooding attack at early stage. The malicious node causes communication delay. But, the introduced algorithm is suitable only for SYN flooding attack.In [7], Flooding Factor based Framework for Trust Management (F3TM) is introduced in MANETs. True flooding approach detects the attacker nodes with the calculation of trust value. But, the Experimental Grey Wolf algorithm takes large amount of time to calculate the trust value.

III. ATTACK DETECTION AND ISOLATION TECHNIQUES FOR MULTIPATH AND MULTICAST ROUTING IN MANET

MANET is an ad hoc network where the nodes are mobile in nature with each other in network management. The key objective of MANET routing protocol is to form efficient route between a pair of nodes where the data packets are delivered in a suitable way. Routing is the method of selecting the best paths in network. Multipath routing is a method that uses essential physical network resources through multiple source-destination paths. Multicasting denotes the forwarding messages to multiple Receivers (R) through Intermediate Receivers (IR). The security of MANETs in group communications is a demanding task because it has multiple sources and multiple destinations.Intrusion Detection System (IDS) is an essential method for detecting different types of attacks. Some of the recent related works regarding the secured routing in MANET are reviewed.

1) Secure Route Discovery in AODV in Presence of Black hole Attack

Route Discovery in AODVhas intrinsicsusceptibility that is exploited throughmalicious node with blackhole attack. Blackhole node maintains short and unexpiredroute fromits routing table through sending fake RREP when the RREQpacket is collected. When the fake RREP messagereceived at source node, route to destination is identified with help of intermediate malicious node. After that, all legalRREP messages from other intermediate and destinationnodes are rejected. Blackhole node attracts the data traffic by fooling sourcenode and drops all the data packets rather thanforwarding. Blackhole node considers the hop count with the low value and destination sequence number to high value in order toincrease the chance ofacceptance at source node.

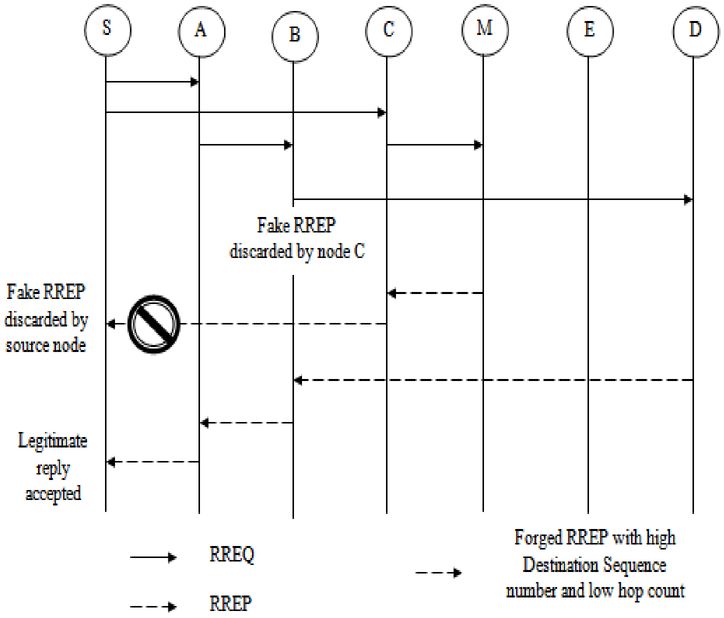
S
A
B
C
M
E
D
Fake RREP discarded by node C
Fake RREP discarded by source node
Legitimate reply accepted
RREQ
RREP
Forged RREP with high Destination Sequence number and low hop count

Figure 1 Secure Route Discovery in presence of Black hole Node

An efficient defense technique against blackhole attack identifies the secure route by improving the packet processing in normal AODV with minimal routing overhead and delay. Then, the packet processing technique of normal AODV performance gets improved by identifying the blackhole attack. The technique needs every node to preserve the blackhole list by listing ID’s of malicious nodes for denoting the status whether fake or legitimate packet. For minimizing the routing overhead and for faster communication, Hello packets are used rather than broadcasting the additional alarm packets when misbehavior is identified as shown in figure 1. ‘‘sendHello’’ and ‘‘receiveHello’’ are employed for sending and retrieving the blackhole list. Hello messages are employed in AODV for distributing the connectivity information. The threshold value is computed depending on number of RREQs sent and

RREPs received. Sequence number get increase while sending new packet by a node. The secure route is selected for sending data packets.

2) Novel technique for node authentication in MANET

A Collection of mobile nodes communicating through wireless links to form a network is called as MANET. Any node joins or leaves the network at anytime. Every node functionsas a router in network and tracks the routing mechanism to communicate with each other. Routing is the process oftransmitting the packet from one node to another node throughpredefined or on-demand path. During routing process, every node cooperates with each other to transmit the data. Much vulnerability present in MANET is wireless links, lack of centralized management, scalability, dynamic topology, cooperativeness, inadequate resources and bandwidth limitations. While transmitting the packets, MANETs are vulnerable to the active and passive attacks by malicious nodes. Toprovide the secure routing bypreventing the Black hole attacks and flooding in MANETs, node authentication has to be carried out for the control packets. The node receives a request or reply packet and validates the initiator tosend it. This mechanism is used for providing authentication with lesser resource utilization.

A node authentication technique is introducedfor MANETs to getcombined with routing protocol and provides security. In this technique,exchange of key is more efficient andreliable for MANETs. Thenode authentication technique is more robust in presenceof malicious nodes and it is multipath communication basedprotocol as described in figure 2.

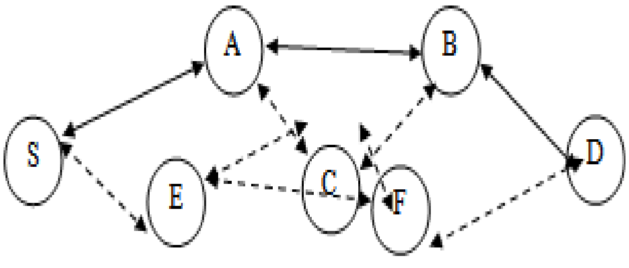

Figure 2 Node Authentication Representation Diagram

The node authentication is carried out with two steps. Initially, each node on network before sending RREQ, it adds ones compliment of its own IP address and originator signs the destination IP address and sends with the public key. Any node enters into network not known that node has increment ones compliment of its IP address, the packets from that particular nodes get dropped by their neighbors. Simultaneously when node fails in authentication, warning message is transmitted over network denoting the existence of malicious nodes with its IP address.

The processing time of additional neighboring nodes receiving packets from malicious node are saved by removing them without any further verification and making the malicious node get separated on network. After receiving the RREQ by destination node,it decrypts with private key. Thereliability of sourceand destination IP address is verified. When the destination identifies any altered transmission, it sends the warning over network otherwise RREP packet is created and transmitted to thesource. The source validates the authentication of destinationafter receiving the RREP.

3) Cross-layer based Multiclass Intrusion Detection System for Secure Multicast Communication of MANET in military networks

The designed IDS architecture comprises three module, namely data collection, detection, and response module as described in figure 3. The data collection module is a cross-layer features that gathers the patterns from MAC as well as routing layer of local and neighbors transmission behavior. The response module generates its counterattack action from routing layer. The observer routing layer starts the essential action to avoid accused node from multicast group. The detection module comprisestwo phases, namely training/learning and testing/validation. In training phase, the classifier model is built through supervised learning with help of class labeled training dataset. In testing phase, the accuracy of model isconfirmed with unknown class label instances.

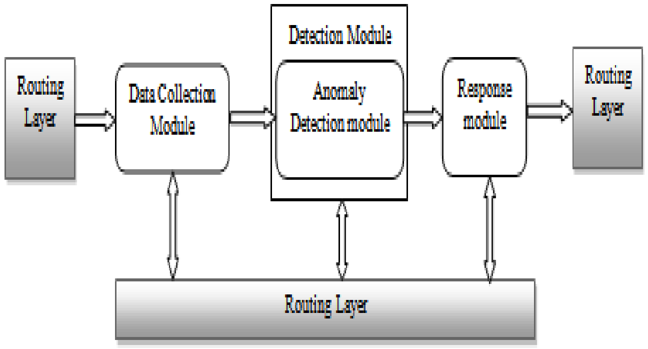

Figure 3 Architecture of Cross-Layer Distributed IDS

In distributed crosslayer IDS, data preprocessing is carried out to improve the quality oforiginal dataset. Three data preprocessingsteps are carried out, namely eliminating the redundantattributes, filling the missing-value attributes and feature subsetselection algorithm.

Missing value attributes are filledthrough unknown label as attributes increases the complexity when the model getsconstructed by classification algorithm. The feature subset selectionalgorithm extracts the relevant features from original dataset. The classifier model in training phase is authenticatedby unidentified class-label dataset. The classifier model predicts the class label for every instance of testing dataset by means of knowledge learnedfrom training phase.Testing dataset comprises subtype of normal, congestion and stealthy attack instancesin variousdistributions. The validation process is carried outto examine the each classifier performance metrics.

IV. COMPARISON OF ATTACK DETECTION AND ISOLATION TECHNIQUES FOR MULTIPATH AND MULTICAST ROUTING IN MANET & SUGGESTIONS

In order to compare the attack detection and isolation techniques for multipath and multicast routing in MANET, number of mobile nodes are taken to perform the experiment. Various parameters are used for attack detection and isolation techniquesfor improving the communication security in MANET.

1) Attack Detection Rate (ADR)

Attack detection rate is defined as the rate at which theattacked node gets detected correctly during the multipath and multicast routing. ADR is defined as the ratio of number of attacked node correctly detected from the total number of mobile nodes.

$$Attack\ Detection\ Rate = \frac{Number\ of\ attacked\ node\ correctly\ detected}{Total\ number\ of\ mobile\ nodes}$$

When the attack detection rate is higher, the method is said to be more efficient.

Table 1 shows the attack detection rate with respect to number of mobile nodes ranging from 10 to 100. Attack detection rate comparison takes place on existing Efficient Defense Technique, Node Authentication Technique and Distributed Cross-layer Intrusion Detection System (IDS). From the table value, it is clear that the attack detection rate usingEfficient Defense Techniques higher when compared toNode Authentication Techniqueand Distributed Cross-layer Intrusion Detection System (IDS).The graphical analysis of attack detection rate is shown in figure 4.

Table 1 Tabulation for Attack Detection Rate

Number of Mobile Nodes (Number)	Attack Detection Rate (%)		
	Efficient defense Technique	Node Authentication Technique	Distributed Cross-layer IDS
10	74	61	55
20	76	63	57
30	79	66	60
40	81	69	62
50	83	71	65
60	86	74	68
70	89	76	71
80	91	79	74
90	93	82	77
100	96	85	80

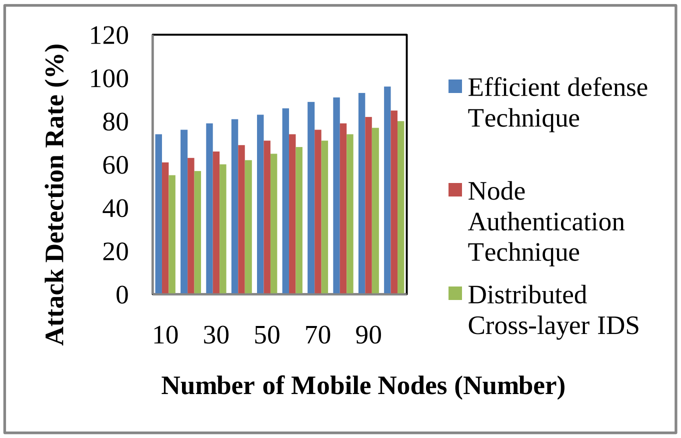

Figure 4 Measure of Attack Detection Rate

As shown in figure 4,attack detection rate during the multicast and multipath routing for different number of mobile nodes areevaluated. Efficient Defense Techniquehas higher attack detection rate than that of Node Authentication Technique andDistributed Cross-layer Intrusion Detection System (IDS).When the number of mobile nodes gets increased,attack detection rate also gets increase correspondingly in all three methods. Research in Efficient Defense Techniqueincreases security level by 17% than Node Authentication Techniqueand 27% higher security thanDistributed Cross-layer Intrusion Detection System (IDS).

2) Security Level during Multipath Routing

Security level is calculated based on the ratio of difference between the data packets being sentand the data packets dropped to the data packet sent during multipath and multicast routing.The mathematical formulation for security is as given by,

$$Security\ Level = \frac{Data\ packets\ sent - Data\ packets\ dropped}{Data\ packets\ sent}$$

When the security level is higher, the method is said to be more efficient.

Table 2 Tabulation for Security Level

Number of Data Packets (Number)	Security Level (%)		
	Efficient defense technique	Node Authentication Technique	Distributed Cross-layer IDS
10	64	78	58
20	66	81	60
30	69	83	63
40	71	86	66
50	73	89	67
60	76	91	71
70	78	93	74
80	81	94	77
90	84	96	80
100	86	97	82

Table 2 shows the security level during multipath routingwith respect to number of data packets ranging from 10 to 100. Security Levelcomparison takes place on existing Efficient Defense Technique, Node Authentication Technique and Distributed Cross-layer Intrusion Detection System (IDS).From the table value, it is clear that the security levelusingNode Authentication Technique is higherwhen compared toEfficient Defense Techniqueand Distributed Cross-layer Intrusion Detection System.The graphical analysis of security level during multipath routing is shown in figure 2.

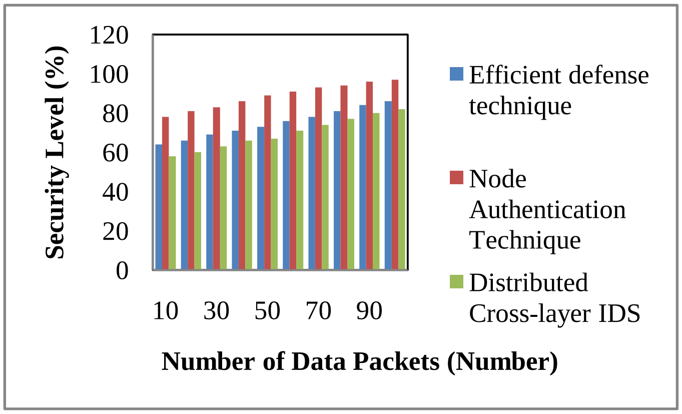

Figure 5 Measure of Security Level

From figure 5, security level during the multicast and multipath routing for different number of data packets areevaluated. Node Authentication Techniquehas higher security level than that of Efficient Defense Technique andDistributed Cross-layer Intrusion Detection System (IDS).When the number of data packets gets increased, the security level gets increased correspondingly in all three methods. Research in Node Authentication Techniqueincreases security level by 19% than Efficient Defense Techniqueand 28% higher securitythanDistributed Cross-layer Intrusion Detection System (IDS).

3) Packet Forwarding Time (PFT)

Packet Forwarding Time is defined as amount of time taken for forwarding the data packets from one node to another node. PFT is the ratio ofproduct of data packetscount and one data packet size to the data packet transferring speed. It is measured in terms of milliseconds (ms). The mathematical formula of packet forwarding time is given by,

$$PFT = \frac{number\ of\ data\ packets * one\ data\ packet\ size}{Data\ packet\ transfering\ speed}$$

When the packet forwarding time is lesser, the method is said to be more efficient.

Table 3 shows the packet forwarding timewith respect to number of data packets ranging from 10 to 100. Packet forwarding time comparison takes place on existing Efficient Defense Technique, Node Authentication Technique and Distributed Cross-layer Intrusion Detection System (IDS).From the table value, it is clear that the packet forwarding time using Distributed Cross-layer Intrusion Detection System (IDS) is lesser when compared toEfficient Defense Techniqueand Node Authentication Technique.The graphical analysis of packet forwarding time during multipath routing is shown in figure 2.

Table 3 Tabulation for Packet Forwarding Time

Number of Data packets (Number)	Packet Forwarding Time (ms)		
	Efficient defense technique	Node Authentication Technique	Distributed Cross-layer IDS
10	48	35	23
20	52	38	26
30	55	41	31
40	58	43	34
50	62	45	36
60	64	48	39
70	67	51	42
80	71	54	45
90	74	57	47
100	77	61	51

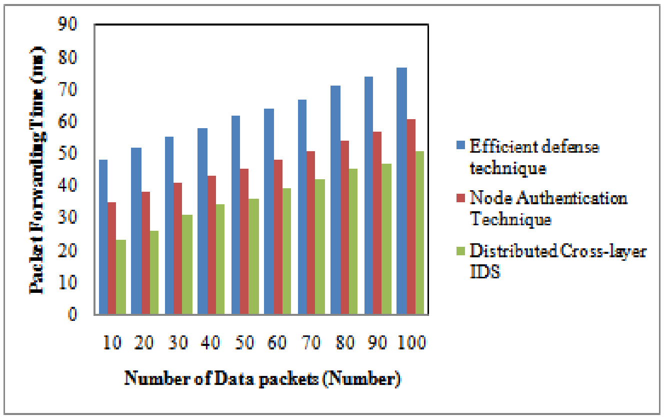

Figure 6 Measure of Packet Forwarding Time

From figure 6, packet forwarding time for attack detection and isolation during the multicast and multipath routing for different number of data packets areevaluated. Distributed Cross-layer Intrusion Detection System (IDS) consumes lesserpacket forwarding time than that of Efficient Defense Technique and Node Authentication Technique.When the number of data packets gets increased, thepacket forwarding time gets increased correspondingly in all three methods. Research in Distributed Cross-layer Intrusion Detection System (IDS)consumes41% lesser packet forwarding time than Efficient Defense Techniqueand 22% lesser packet forwarding timethan Node Authentication Technique.

V. DISCUSSION ON LIMITATION OF ATTACK DETECTION AND ISOLATION TECHNIQUES FOR MULTIPATH AND MULTICAST ROUTING IN MANET

The node authentication technique introduced for MANETs will provide security. The designed technique is robust in presence of malicious nodes. It acquires minimal computation overhead and the resources are constraints. The present technique achieves higher performance with secure routing. However, performance in terms of throughput, delay and packet delivery ratio is ineffective on large area networks.The efficient defense technique discoversthe secure routefor data transmissionby implementing packet processing technique in AODV with minimum routing overhead and delay. Single malicious node improves the network performance with defense technique and detects the multiple blackhole attack with help of their neighbors and isolated nodes.However, end to end delay was maximized as malicious nodes move away from source node.

A new indirect internal stealthy attack and known direct internalstealthy attacks like black hole and deny-to-forwardattacks were discussed on tree-based multicast routing protocol.A distributed cross-layerbased machine learning anomaly detection system is used formulticast communication of MANET. It is not easy to find the correlation between two sets of attributes formulticlass classifier. The accuracy, cost and delay of distributed cross-layer IDS are calculated. However, the black hole and deny-to-forwardattacks are only detected and isolated.

1) Related Works

A Composite Trust-based Public Key Management (CTPKM) designed in [8]with minimal susceptibility.An optimal trust threshold attains the objectives between the performance and security through inherent tradeoffbetween the trust and risk. However, the attack is not identified during the security process that results in lesser security level. A secure and energy-efficient stochastic multipath routing protocol designed in [9] with help of Markov chain for MANETs. Though the energy consumption is reduced, the security level is not increased.The standard ad hoc on-demand multi-path distance vector protocol is extended as base routing protocol in [10]. However, the Dolphin Echolocation

Algorithm not exactly identified the malicious node through classification process.

A combined approach of Fuzzy Trust Based Clustering (FTBC) and hierarchical distributed group key management isintroduced in [11]. But, the packet forwarding time is not reduced by using fuzzy trust based clustering and hierarchical distributed group key management. Node isolation attackis a major attack in Optimized Link State Routing protocol (OLSR) in [12]. A novel solution defends OLSR protocol from node isolation attack through identifying similar tactics by attack itself. But, the attack isolation rate was not increased.

2) Future Direction

The future direction of survival study is to improve the communication security for detecting and isolating the attacks during the multipath and multicast routing by using the secured routing techniques in MANET.

VI. CONCLUSION

A comparison of different techniques for attack detection and isolation during the multipath and multicast routing is studied. From the survival study,theattack detection is not carried out in efficient manner as the techniques detect only one type of attack. In addition, the communication security level is not improved by means of existing techniques.The packet forwarding time during multipath and multicast routing is not reduced beyond certain level.The wide range of experiments on existing methods and algorithm evaluates thecomparative results of various attack detection and isolation techniqueswith its limitations. Finally from the limitation identified from the existing works, further research work can be carried out for attaining improved communication security during routing process in MANET.

References

[1] Gautam M. Borkar and A. R. Mahajan,“A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks”, Wireless Networks, Wireless Networks, Springer, Pages 1–18

[2] Geetha K. and N. Sreenath, “Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol”, Arabian Journal for Science and Engineering, Springer, Volume 41, Issue 3, March 2016, Pages 1161–1172

[3] Gomathi K., B. Parvathavarthini and C. Saravanakumar, “An Efficient Secure Group Communication in MANET using Fuzzy Trust Based Clustering and Hierarchical Distributed Group Key Management”, Wireless Personal Communications, Springer, Volume 94, Issue 4, June 2017, Pages 2149–2162

[4] Jaspal Kumar, M. Kulkarni, Daya Gupta and S. Indu,“ Secure route discovery in AODV in presence of blackhole attack”, CSI Transactions on ICT, Springer, Volume 3, Issue 2–4, December 2015, Pages 91–98

[5] Jin-Hee Cho, Ing-Ray Chen and Kevin S. Chan, “Trust threshold based public key management in mobile ad hoc networks”, Ad Hoc Networks, Elsevier, Volume 44, July 2016, Pages 58-75

[6] Malik N. Ahmed, Abdul Hanan Abdullah, Hassan Chizari and Om prakash Kaiwartya, “F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs”, Journal of King Saud University - Computer and Information Sciences, Elsevier, Volume 29, Issue 3, July 2017, Pages 269-280

[7] Menaka Pushpa Arthur and Kathiravan Kannan,“ Cross-layer based multiclass intrusion detection system for secure multicast communication of MANET in military networks”, Wireless Networks, Springer, Volume 22, Issue 3, April 2016, Pages 1035–1059

[8] Nadav Schweitzer, Ariel Stulman, Asaf Shabtai and Roy David Margalit,“Mitigating Denial of Service Attacks in OLSR Protocol using Fictitious Nodes”, IEEE Transactions on Mobile Computing, Volume: 15, Issue 1, January 2016, Pages 163 – 172

[9] Reshmi. T. R. and K. Murugan, “Secure and Reliable Auto configuration Protocol(SRACP) for MANETs”, Wireless Personal Communication, Springer, August 2016, Volume 89, Issue 4, Pages 1243–1264

[10] Sajal Sarkar and Raja Datta, “A secure and energy-efficient stochastic multipath routing forself-organized mobile ad hoc networks”,Ad Hoc Networks, Elsevier, Volume 37, Part 2, February 2016, Pages 209-227

[11] Srinivas Aluvala, K. Raja Sekhar and DeepikaVodnalaca, “A novel technique for node authentication in mobile ad hoc networks”, Perspectives in Science, Elsevier, Volume 8, 2016,Pages 680—682

[12] Usha.G, M. Rajesh Babu and S. Saravana Kumar, “Dynamic anomaly detection using cross layer security in MANET”, Computers and Electrical Engineering, Elsevier, Volume 59, April 2017, Pages 231–241.