TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 14601 - 14608

Secure Cluster based Certification Revocation AOMDV Protocol in Mobile Ad-Hoc Network

Dr. K Madhuri
Professor, Dept. Of CSE, Neil Gogte Institute of Technology, Hyderabad, Telangana, India.

Article Info
Volume 82
Page Number: 14601 - 14608
Publication Issue:
January-February 2020

Article History
Article Received: *18 May 2019*
Revised: *14 July 2019*
Accepted: *22 December 2019*
Publication: *28 February 2020*

Abstract:
The mobile nodes are included in Mobile Ad-hoc Network (MANET) in which the role of a router and terminal are played by respective mobile nodes. The packet for reaching the destination is ensured by selecting a reliable routing protocol although it is acting as a router and the packet transmission is done by an agent whenever it performs as a terminal. This paper considers the existing procedure for transmitting the secure packet within the MANET with Ad-hoc On Demand Multipath Distance Vector (AOMDV) routing protocol. Selecting the routes or initializing the denial-of-service attacks is affected by permitting the attacker nodes by the subjecting various attacks to the existing adhoc routing protocols. Particularly, the black hole wherein the packets are attracted by malicious nodes is implemented and it is not allowed in reaching the destination. The packets within the hostile MANET environment is secured by a protocol named as AOMDV and ECC. The malicious nodes are detected and avoided by implementing this approach accompanied by intrusion detection system (IDS). Novel cluster secure certificate revocation approach is proposed in this network. The clusters are formed by dividing the network effectively for distributing the keys amongst the nodes. The CH nodes are provided with the key distribution as well as verification procedure. Moreover, the malicious nodes keys are revoked by introducing the certificate revocation process. Furthermore, the residual nodes are not contacted by the malicious nodes by excluding the valid keys.Network simulator-2 is used to simulate the network schemes.

Keywords:*MANET, AOMDV, Elliptic Curve Cryptography, Black hole Attack, SAOMDVECC, NSCR.*

I. INTRODUCTION

A multi-hop radio network is formed within an infrastructure less environment by MANET which collects specific mobile nodes that communicate with one another. The role routers as well as terminals are played by the nodes in MANETs. Additionally, the wired networks and the routing path in ad-hoc networks are not similar to each other. The ad-hoc networks don't involve certain safety methods that are designed on behalf of the wired topology [1].

The establishment of the secured ad-hoc routing protocols [2] is very complex due to the varying topology and the flexible performance of the mobile nodes. In the transmission range, the entire nodes collect the data that is transmitted by node. The MANET routing protocol is projected towards various malicious attacks due to the lack of safety in ad-hoc network.

The role of host as well as a router is played by every single node in MANET. A wireless local area network is formed whenever data is received by cooperating with one another. Moreover, several disadvantages take place in addition to these significant characteristics. Certainly, certain severe limitations upon the network safety of topology of the network, routing as well as data traffic are imposed by the above mentioned uses. For example, the operations within the network may fail due to the disruption of the routing procedure [3] by the presence and collaboration of malicious nodes in the network.

The MANETs safety is focused by various investigation works. Every mischievous node is combated by preventing and detecting most of those methods. Additional disturbing damages are caused for the network by initiating a collaborative attack due to the collision of several malicious nodes which in turn weakens the network efficiency. The safety concerns are not considered in the early designing

January - February 2020
ISSN: 0193 - 4120 Page No. 14601 - 14608

process of MANETs rather the routing protocols considered a consistent as well as trusted environment. Compared to blackhole attack, this paper considered a security of AOMDV (Adhoc On-Demand Multipath Distance Vector) protocol in addition to a multipath extension of the AODV routing protocol.

The network packet is forwarded towards the destination by the construction of the routes where each mobile node is working as a router. Every network faces certain challenges in providing secured transmission as well as communication. Nevertheless, the problems of distribution of incorrect routing data, packet dropping as well as selective forwarding are caused within the network due to which various attacks such as black holes or grey holes attack, rushing attack, wormhole attacks [4] are caused.

Various complex applications such as exchanging of messages between groups of soldiers within the battlefield, earthquake alarming, video conferencing and so on using one-to many communications [5]–[9] are supported by MANETs. The distribution of the packets is performed between each other by the destination nodes where the effective communication paradigm is served by the Cooperative multicast. Actually, because of the limited power resource, the packet transmission is refused by the destination node as they act greedily. Therefore, considering the cooperative nature of destination nodes within the multicast scheme design is very complex for a capable support of upcoming multicast-intensive applications within MANETs [10]-[13].

If the entire destination nodes are ready for sharing the packets with one another or when no nodes is ready for sharing the packets with one another, the available investigations focus upon the cooperative multicast in MANETs. In [14]—[17], the non-cooperative multicast method is investigated within two-hop relay MANETs and the simple independent and identically distributed (IID) mobility model is considered in [14-16] and additional general speed-restricted mobility models are considered in [17]. Within the IID mobility model [18], [19], the exploration of the complete cooperative multicast method is done with the two-hop relay MANETs. In cognitive radio MANETs [20], the examination of the comprehensive cooperative multicast methods is done in recent times where the exploitation of spectrum that is allotted for the licensed nodes within the opportunistic manner is performed.

II. Literature Survey

A wireless communication network that doesn't depends upon some of the centralized management or a pre-existing infrastructure is referred as MANET. This method adopts several key managing consultants that are dispersed over a network which is updated in a periodical way by the distribution of secure key. Therefore, the MANET's dynamic environments adopted various efforts of the tasks of the key management authority and the MANET nodes are provided with the certain responsibilities. The constantly developing requirements are achieved by deploying several cryptographic methods and unique security mechanism of the device is compelled on behalf of MANET. By excluding the intrusion due to the illegal causes, the data transmission is protected by permitting the individual as well as corporate entities. Symmetric key cryptography or asymmetric key cryptography or hash functions can be used for the Cryptographic techniques. In MANETs, the development of a new mutual authentication as well as key management (agreement) method was done on behalf of one hop communication. Mutual authentication, confidentiality, integrity as well as key agreement are the various significant characteristics. Generation of RSA signature in addition to verification procedure [21] are used by the protocol. Depending upon the MANETs, various intelligent methods were appeared by several investigators from the past few decades. Compared to wired or infrastructure-based wireless network, safety is considered as the best concern since MANETs are susceptible to the attacks. It is a complex thing to design an efficient security protocol for MANET. Distributed broadcast radio channel, uncertain operating atmosphere, central authority deficiency, association deficiency between the users, restricted accessibility of resources, in addition to physical vulnerability are the exclusive features of MANETs. With the calculation of performance metrics like packet delivery ratio, end to end delay and throughput [22],

January - February 2020
ISSN: 0193 - 4120 Page No. 14601 - 14608

this paper presents the simulation grounded investigation of the neighbor attack and black hole attack effect upon AOMDV routing protocol. The deterrence in contrast to the routing misbehaviour by the malicious attacks are detected and provided by the presented security scheme [23]. The performances of AOMDV, Attack in addition to IDS scheme are compared in this method. The presented method i.e., IDS method and general multipath routing performances are similar. The efficiency of the overall routing is degraded by the attacker and however, it is detected that this method blocks the routing misbehaviour and 95 % of data is recovered. The key management scheme's categorization within the sensor networks that defines the comparisons as well as the variations are presented in [24]. A new dynamic key management method which is a localized combinatorial keying (LOCK) is described in this paper and the safety as well as the performance is compared using a representative static key management method. At last, the directions of the future research are outlined.

A new key managing method which uses symmetric as well as asymmetric key procedures is presented in [25] and however, a frequency-based method is used to achieve the fundamental updates. Data privacy, key distribution and so on are the various key management aspects provided by this method. Within the key managing procedure as well as the ability of withstanding the attacks intended for the malicious key updates, the proposed method is recognized as the secured process with the discussions of the existing problems.

The loop-free as well as disjoint multiple paths are ensured by the AOMDV key in [26]. A flood-based method maintains the route discovery. For maintaining disjointness as well as loop-freedom, the implementation of AOMDV route update rules is performed on behalf of each node. Various paths amid source as well as destination are found by the protocol. Whenever a route failure is occurred, the additional route is occupied instantly in order to transmit the data. The distribution of the keys between the valid nodes is performed within MANET with the help of ECC. Public and private keys are used in order to encrypt and decrypt the data. Therefore, the details regarding the additional nodes is known to every single node and the data transmission is performed among the nodes is done safely. Excluding the shared secret keys, the original information is unrevealed as encrypted by the malicious node although after the attack.

III. Proposed System

For enhancing the node identity in which the certificate's encryption and decryption may occur and for identifying the documentation validity of secured transmission that takes place over the symmetric cryptography method's application and to distribute the keys efficiently among the nodes, the implementation of a revocation procedure-built secure communication and a certificate cancellation method is done. Each node is provided with the key distribution as well as verification process. Moreover, the keys of the malicious nodes are revoked by the introduction of the certificate revocation process. The communication between the malicious nodes and residual nodes may not be performed excluding the valid keys. This paper introduces NSCR (New secure certificate revocation scheme) on behalf of MANET. Mainly, the selection of CH is done depending upon the distance amid the nodes and the collection of nodes (mobile users) is done within several clusters. The selection of node with a least distance is done for selecting the CH out of the cluster. Collecting the data out of the cluster members as well as grouping them within the clusters is the objective of CH. Therefore, the entire message's reliability is validated by the transmission of trusted messages only with the total members of the cluster. The cancelling as well as allocating of the certificates which are belonging to the mobile users is the responsibility of CA (certificate authority). The particulars of the certificates for the intermediate nodes that are called as receiver are sequentially broadcasted by CA. The transmission of the broadcasted detail towards the respective neighbouring node which is in the vicinity of it is done. Therefore, the nodes are attacked by the certificates or key transmission between the nodes. Until the validity is present, the certificate is lost by the attacked node's avoidance. For picking the revoked nodes out of the cluster, the standards must be followed and the CRL (certificate revocation list) preserves the attacked (revoked) node. The CRL adds the certificates of the nodes that are assumed as

January - February 2020
ISSN: 0193 - 4120 Page No. 14601 - 14608

malicious or suspicious. The CA maintains the CRL data. The CA accumulates the node identities that are revoked and it is transformed within the single value using the collector named as universal accumulator.

Earlier to the expiration of the duration, the attacked nodes are revoked occasionally by CA including the certificates.

The non-membership witness is sequentially verified by the accumulator and a certificate not over-ridden its validity period is guaranteed by it. Whenever, the relating non-membership witness is obtained, the legitimacy of a provided certificate is validated by the ability of the usage of accumulated measure with the entity of the network. Rather than directing it towards the overall nodes within the cluster, the valid certificate is issued by CA to CH. The aggregated measure of group of witness nodes (active nodes) is preserved and the ids of the revoked nodes are measured by each CH that operates as a MR (mobile repositories). The CH is requested by the cluster members whenever there is a requirement for data. With the help of symmetric cryptography application method, the data is transmitted safely once the particulars are attained from CH and the encryption and decryption of the certificates might take place. The block diagram of our proposed method is depicted in Figure 1.

Trusted Authority (TA): TA is a private 3rd party that performs the generation of structure factors, principal public key, secret key, and secret key participants, preloading them into the mobile users, as well as tracing the users from their virtual characteristics during any malpractice.

This method involves 6 phases mainly.

1. **Setup:** here, the TA generates the system parameter's loading within the tamper proof devices of the nodes.
2. **Anonymous identity generation:** Here, a similar secret key is generated by hiding the actual identity whenever a registered pseudo identity is received.
3. **Certificate authority:** the responsibility of distributing as well as revoking the certificates belonging to the nodes is performed by this phase. The intermediate nodes which are assumed as the hop node by TA receive the certificate details. The broadcasting details within its coverage area are received by respective neighbour node.
4. **Message generation:** this phase uses a timestamp t that is used in the transmission of computed message to the hop node by selecting a message.
5. **Verification of messages by hop node:** here, a hop node is used to verify the identity as well as the reliability of received messages. The validation of the entire messages is done whenever the messages that are trusted by the entire members are transferred by the related-neighbor node.
6. **Verification of hop nodes' output by Destination node:**with the help of the outcomes obtained out of the hop nodes, the detection of false results as well as revoke mischievous hop nodes is done and the destination nodes within this stage is verified. The standards must be followed for preserving the attacked (revoked) node in CRL by picking the revoked node from the network area. The CRL moreover adds the certificates of the malicious or malicious nodes.

January - February 2020
ISSN: 0193 - 4120 Page No. 14601 - 14608

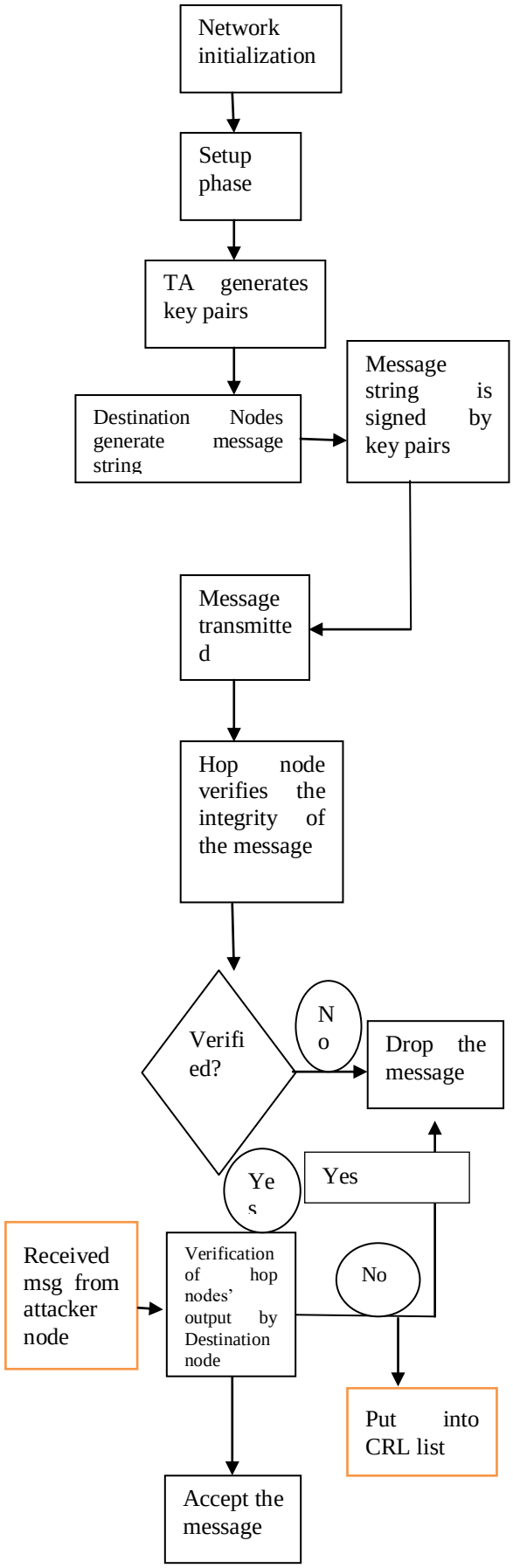

Fig1: Flowchart of Proposed system

IV. Results And Discussion

Network simulator NS2 is used to perform the performance assessment and also compares the proposed method, NSCR with the novel SAOMDV-ECC and AOMDV. The Energy consumption (EC), Average End to End Delay (E-to-E Delay), and Throughput (Thr) are compared and their performances are assessed with the help of parameters.

TABLE 1
Simulation parameters.

PARAMETER	VALUE
Application traffic	CBR
Transmission rate	1000 bytes/ 0.1ms
Radio range	250m
Packet size	1000 bytes, 1500 bytes
Attacker	1
Routing Protocol	AOMDV
Simulation time	10s
Number of nodes	25
Area	800 x541
Malicious nodes	NSCR, SAOMDV-ECC, AOMDV
Transmission Protocol	UDP

The proposed method is analysed and investigated using Network Simulator (NS2) version 2.35. Within a region of 800 x 541 m^2, 25 nodes are deployed in the simulation framework. The implementation of Random Way Point (RWP) mobility is done and the range of 250m is set for the transmission of the ideal unstructured. In accordance with UDP protocol, the implementation of 2 scripts is done in which generation of traffic for CBR is the initial one. On behalf of the overall investigations, Simulation time is set to 10 sec.

The routing data is supported by the routing protocol (AOMDV) in this simulation process and moreover, the data is distributed among the entire nodes within the network simulation.

January - February 2020
ISSN: 0193 - 4120 Page No. 14601 - 14608

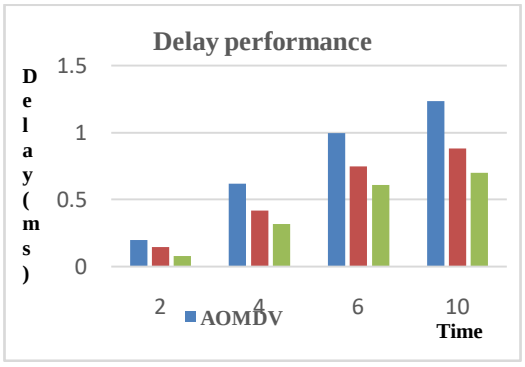

Figure 2: End to End Delay

The end2end delay is presented in the above graph and simulation time versus delay is shown here. Compared with the AOMDV with ECC and normal AOMDV routing protocol, the novel secure certificate revocation method's performance is enhanced by reducing the delay among the nodes.

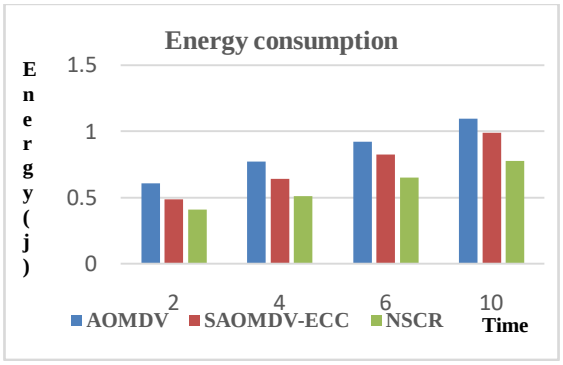

Figure 3: Energy Consumption

The energy consumption is shown in the above graph and simulation time versus energy is shown. In comparison with the secure AOMDV with ECC and normal AOMDV routing protocol, the energy values are improved by the novel secure certificate revocation method's performance.

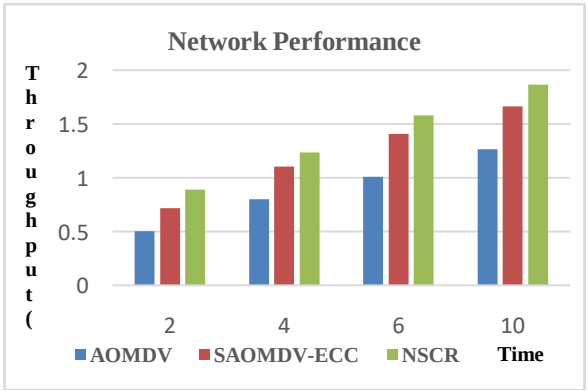

Figure 4: Throughput

Simulation time versus throughput graph is shown in the above figure and throughput is also presented. Corresponding with the secured AOMDV using ECC and normal AOMDV routing protocol, the throughput is improved by the efficiency of novel secure certificate revocation method.

V. Conclusion

The route selection is affected and the denial-of-service attacks are initialized by permitting the several attacker nodes in attacking the existing adhoc routing protocols. Particularly, the blackhole attack is employed wherein the packets are attracted by the malicious nodes and are avoided in reaching the destination. A resolution is provided by AOMDV and ECC in order to secure the packets within the environment of hostile MANET. The malicious nodes are detected and avoided by implementing intrusion detection system (IDS) and the proposed method. Certificate revocation technique is proposed in this network. The distribution of network is done within various clusters for distributing the keys efficiently among the nodes. The CH nodes are provided with key distribution as well as verification process. Moreover, the keys of malicious nodes are revoked by introducing the certificate revocation procedure. The residual nodes are not contacted by the malicious nodes by excluding the valid keys. In comparison with the existing AOMDV as well as SAOMDV-ECC, an efficient method is detected for NSCR corresponding to the simulation results that are conducted for the discussed parameters.Network simulator-2 is used in this paper for the simulation of the network considerations.

VI. References

[1] L. Shi-Chang, Y. Hao-Lan and Z. Qing-Sheng, "Research on MANET Security Architecture Design," 2010 International Conference on Signal Acquisition and Processing, Bangalore, 2010, pp. 90-93.doi: 10.1109/ICSAP.2010.19

[2] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," 10th IEEE International Conference on Network Protocols, 2002. Proceedings., Paris, France, 2002, pp. 78-87.

January - February 2020
ISSN: 0193 - 4120 Page No. 14601 - 14608

[3] J. Chang, P. Tsou, I. Woungang, H. Chao and C. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," in IEEE Systems Journal, vol. 9, no. 1, pp. 65-75, March 2015.doi: 10.1109/JSYST.2013.2296197.

[4] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc network," in Proc. CNDS'02, 2002, p. 1-13.

[5] S. Shakkottai, X. Liu, and R. Srikant, "The multicast capacity of large multihop wireless networks," IEEE/ACM Transactions on Networking, vol. 18, no. 5, pp. 1691–1700, October 2010.

[6] Z. Qian, X. Tian, X. Chen, W. Huang, and X. Wang, "Multicast capacity in MANET with infrastructure support," IEEE Transactions On Parallel and Distributed Systems, vol. 25, no. 7, pp. 1808–1818, July 2014.

[7] Z. Li, C. Wang, C. Jiang, and X. Li, "Multicast capacity scaling for inhomogeneous mobile ad hoc networks," Ad Hoc Networks, vol. 11, no. 1, pp. 29–38, January 2013.

[8] S. Zhou and L. Ying, "On delay constrained multicast capacity of largescale mobile ad-hoc networks," in INFOCOM, 2010.

[9] J. P. Jeong, T. He, and D. H. C. Du, "TMA: Trajectory-based multianycast forwarding for efficient multicast data delivery in vehicular networks," Computer Networks, vol. 57, no. 13, pp. 662–672, September 2013.

[10] X. Ge, J. Yang, H. Gharavi, and Y. Sun, "Energy efficiency challenges of 5G small cell networks," IEEE Communications Magazine, vol. 55, no. 5, pp. 184–191, May 2017.

[11] T. Han, X. Ge, L. Wang, K. S. Kwak, Y. Han, and X. Liu, "5G converged cell-less communications in smart cities," IEEE Communications Magazine, vol. 55, no. 3, pp. 44–50, March 2017.

[12] X. Ge, S. Tu, G. Mao, C. Wang, and T. Han, "5G ultra-dense cellular networks," IEEE Wireless Communications, vol. 23, no. 1, pp. 72–79, February 2016.

[13] Z. Su, Q. Xu, Y. Hui, M. Wen, and S. Guo, "A game theoretic approach to parked vehicle assisted content delivery in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, DOI: 10.1109/TVT.2016.2630300.

[14] B. Yang, Y. Cai, Y. Chen, and X. Jiang, "On the exact multicast delay in mobile ad hoc networks with f-cast relay," Ad Hoc Networks, vol. 33, pp. 71–86, October 2015.

[15] X. Wang, W. Huang, S. Wang, J. Zhang, and C. Hu, "Delay and capacity tradeoff analysis for motioncast," IEEE/ACM Transactions on Networking, vol. 19, no. 5, pp. 1354–1367, October 2011.

[16] C. Hu, X. Wang, and F. Wu, "Motioncast: On the capacity and delay tradeoffs," in MobiHoc, 2009.

[17] X. Wang, Y. Bei, Q. Peng, and L. Fu, "Speed improves delay-capacity trade-off in motioncast," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 729–741, May 2011.

[18] X. Wang, Q. Peng, and Y. Li, "Cooperation achieves optimal multicast capacity-delay scaling in MANET," IEEE Transactions on Communications, vol. 60, no. 10, pp. 3023–3031, October 2012.

[19] J. Liu, X. Jiang, H. Nishiyama, and N. Kato, "Multicast capacity, delay and delay jitter in intermittently connected mobile networks," in INFOCOM, 2012.

[20] J. Zhang, Y. Li, Z. Liu, F. Wu, F. Yang, and X. Wang, "On multicast capacity and delay in cognitive radio mobile ad hoc networks," IEEE Transactions Wireless Communications, vol. 14, no. 10, pp. 5274–5286, March 2015.

[21] Vandana Arora, Mr. Sunil Ahuja, " Trusted key management with RSA based Security Policy for MANETs", Intenational journal of Advance research, ideas and Innovations in Technology, Volume 2, Issue 3, 2016.

[22] Priyanka Bansal, Anuj K.Gupta, " Impact of Black Hole and Neighbor Attack on AOMDV Routing Protocol", International journal of

January - February 2020
ISSN: 0193 - 4120 Page No. 14601 - 14608

Innovations in Engineering and Technology, Vol.3, Issue 4, April 2014.

[23] S Shrivastava MANET", International Journal on AdHoc, C Agarwal, A. Jain, " An IDS scheme against black hole attack to secure AOMDV routing in Networking Systems, (IJANS) Vol. 5, No. 1, January 2015.

[24] Young-Sik Hwang, Seung-Wan Han and Taek-Yong Nam, "The expansion of key infection model for dynamic sensor network," 2006 8th International Conference Advanced Communication Technology, Phoenix Park, 2006, pp. 5 pp.-511.doi: 10.1109/ICACT.2006.206018.

[25] A. Boukerche, Y. Ren and S. Samarah, "A Secure Key Management Scheme for Wireless and Mobile Ad Hoc Networks Using Frequency-Based Approach: Proof and Correctness," IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, New Orleans, LO, 2008, pp. 1-5.doi: 10.1109/GLOCOM.2008.ECP.353.

[26] Jeenat Sultana, Tasnuva Ahmed, "Securing AOMDV Protocol in Mobile Adhoc Network with Elliptic Curve Cryptography", International Conference on Electrical, Computer and Communication Engineering (ECCE), February 16-18, 2017, Cox's Bazar, Bangladesh.