I J C T A, 10(20), 2017, pp. 41-52 ISSN: 0974-5572

A Novel Secure and Efficient Clustering Based Routing Protocol for Manet with Certificate Revocation

Shajan Joseph* and A. Rajaram**

ABSTRACT

The MANET have the ability of moving that is in the network any number of nodes can join and move anywhere and then depart from the model. This leads to high possibility of violating the security of the network model and thus the malicious nodes can access the information of another node. With this motivation, to avoid the security problem a new cluster based routing scheme is projected to produce more security to the network. Previously, Cluster based Neighbor Coverage Routing Scheme is proposed to improve the load balancing and network connectivity in MANET where the security problem is not done. So, in this work, implemented with an improvement on cluster based routing protocol using clustering algorithm called Restructured network based unclear logic for the valid routing path across cluster heads under two restraints such as cluster head node degree and hop count. This protocol can be more efficient and has low energy consumption and low cluster head death even for larger region. In addition to that certificate revocation with the certificate verification and validation technique is utilized to advance the security of MANET. The verification entails preserving secure connections against spoofing attacks and invalid certificates and in terms of the certificate validation, checks the certificate of the recipient to make sure its identity. Finally, certificate revocation is utilized to disconnect the malicious nodes from the network. It is not possible to communicate that malicious node with any other nodes when the token of the malicious node is revoked in the network and thus the security and the reliability of the MANET are enhanced. In addition to that, the Cluster-to-Cluster communication is also possible in a secure manner. The performance of the proposed method is compared with previous protocols such as the NCPR, and also the CLMNRP. The experimental results showed that the proposed RNULVRP attains better performance than other existing cluster based protocols.

Keywords: Cluster-Based Routing Protocol, Certificate Verification and Validation, Revocation, Authentication, MANET, Security, Restructured network based unclear logic.

1. INTRODUCTION

A MANET may be a localized network within which all network activities just like the finding the topology and packets receiving are managed by the nodes themselves the mobile nodes are related to the task of routing packets. Manets are a lot of sensitive to numerous sorts of security attacks [1, 2] because of their often varied wireless nature. To ensure secure network services may be a major challenge related to any MANET [3]. Thus security in MANET is one among crucial demand and implementing security [4, 5] is so a major importance in such sort of networks.

The primary concern is to supply protected communications among mobile nodes during hostile surroundings, by preventing or detecting the attacker who will launch attacks to disrupt network security. Among security problems in Mobile ad hoc network, certificate management is a wide used mechanism that is a method of transference trust [6, 7], that secure the applications and network services. The right answer for certificate management encompasses three elements specifically detection, interference, and revocation. And plenty of researchers have created outstanding achievements during this area.

* Research Scholar, Anna University, Chennai, India, *Email: gct143@gmail.com*

** Professor, Department of Electronics and Communication Engineering, EGS Pillay Engineering College, Nagapattinam, India, *Email: shajanjoseph27@gmail.com*

Certificate revocation may be a requirement in securing network communications which could be a part related to Certificate Management that could be a wide accepted technique to supply trustworthy public key infrastructure for each application security and network service security. The three phases required in Certificate Management are prevent, detect and relocated. Many works are originated that suggests the way to take away malicious attacks within the network. It is vital that any attack ought to be known as shortly as attainable. Certificate revocation may be a major task wherever listing and removing the certificates of nodes that are detected to launch attacks on the neighborhood, is done.

A node ought to be off from the network and discontinue from all its activities right away once it is found as misbehaved. One among the key challenges of a cluster based routing protocol is that the appointment of a skillful cluster head. The cluster head will be selected also by allowing for solo performance metric or multiple performance metrics. Multiple metrics based clustering schemes performs higher than the single metric based clump scheme thence it takes multiple parameters like node's degree, mobility, energy, bandwidth, etc.

Therefore, during this proposed clustering protocol, have to take multiple performance factors for the selection of primary and secondary cluster head. Another vital issue of cluster based routing is to scale back the routing overhead. The cluster heads and gateway nodes are flooded with route request with route reply packets during the route discovery phase. Therefore, because of the character of high mobility of ad hoc networks, any intermediate CH or gateway might move during the route reply method. So as to scale back the routing overhead and to deal with the cluster head mobility, proposed an adaptive Restructured network based routing protocol to facilitate route discovery and maintenance and to boost network stability.

The contribution of the paper is planned as follows: In Section –II, an outline of previously connected works was conferred. Section-III consists of the summary of the projected solution and also the estimation of metrics that are chosen for the projected clustering protocol was mentioned. Section-IV shows the performance analysis of our projected work. Section V concludes the paper and offers directions for the future scope.

2. RELATED WORK

GSR Emil Selvan et al [8] proposed a malicious node detection scheme in network environment. The projected approach relies on threshold cryptography and Chinese remainder theorem. All nodes involved with the transmission method are genuine. Then, threshold cryptography is employed to share the message and Chinese remainder theorem for routing verification and to validate whether or not the node is genuine or not.

S.M. Sarwarul Islam Rizvi et al [9] projected security module supported threshold cryptography for shielding the mobile agent and agent server in an ad hoc network. The brink cryptography could be a new environment within the cryptographic world wherever trust is distributed among multiple nodes within the network. The present approach provides key protection schemes such as privacy, honesty and hopness. Sanjay Raghani et al [10] projected the design of distributed CA supported threshold cryptography for mobile unexpected networks. The projected protocol is extended with a group of observation protocols by providing dynamic behavior.

Keun-ho lee et al [11] projected authentication protocol supported hierarchical Clusters in unexpected Networks (AHCAN). The projected scheme designs an end-to-end authentication protocol that depends on mutual trust between nodes in different clusters. Pushpita Chatterjee [11] described a game theoretic routing model. Two mechanisms Credit and name are to force the nodes to figure honestly. This model primarily projected to beat the matter of ungenerous behavior of node, wherever the node behaves idle and stop the transmission.

M. Jiang et al. [12] described Cluster-based routing protocol (CBRP). In CBRP cluster based mostly routing protocols nodes are organized to make cluster. Every cluster contains a cluster-head, which

coordinates the information transmission among the cluster and to different clusters [13]. In CBRP routing data is transferred through cluster head solely, therefore the quantity of management overhead carried through the network is much less as compared to the convention flooding techniques.

Mohamed Dyabi et al [14], propose a new clustering algorithm for ad hoc networks, wherever the clusters are shaped around the most powerful nodes, i.e. The node that has the most effective material resources corresponding to residual energy, free memory, processor speed and hard disk space is elective as cluster head. 2ACK [15] projected the scheme to police investigation misbehaving links instead of misbehaving nodes. During this packet has been appointed route of two hops that is in other way and disadvantages is higher routing overhead because of transmission of 2ACK to the supply nodes.

Subbian Umamaheswari et al [16] propose an anthocnet + Security (ANTSEC) framework that features an increased cooperative caching theme embedded with artificial scheme. Network structure enhances protection by injecting attacks into the packet informations, improves the packet delivery ratio and reduces end-to-end delay by means of cross layer design. S. Talapatra et.al.[17] projected algorithm for cluster head selection and cluster maintenance and this algorithm use selforganising principle for binding a node with cluster which might scale back the explicit message passing in cluster maintenance. The disadvantage of this technique is to that does not elect the cluster head dynamically and needs a lot of messages throughout transferring information.

Chin Yang et al [18] projected a specification based an intrusion detection system for AODV protocol it analyzes the vulnerability, attacks against AODV protocol that manipulate the routing message. It uses the finite state machines for requiring it to correct AODV routing performance and distributed network monitors for attack investigation run time destruction of specification. Minakshi et.al [19] projected an Enhanced HMAC-method for securing the AODV protocol and increasing struggle to key look for injuries and providing verification in addition as integrity.

As per explained in section II the problems involved with the MANET are security, mobility, open medium, dynamic ever-changing topology, lack central observation and administration. These factors are liable for suffering attacks in mobile Ad-hoc network. An accessibility of network services, confidentiality and integrity of information may be achieved by via routing protocols. With the assistance of routing protocol and via certificate revocation algorithms to boost the safety provides high potency of securing the information over the Wireless Network.

3. PROPOSED METHODOLGY

In this section, introduce the cluster based secure routing method through certificate revocation. This method assumes that each one the mobile nodes have gotten their valid certificates from the Certificate Authority (CA). Every node must get the valid certificate type CA to communicate with other nodes. The certificate is that the requirement within which the general public key is guaranteed to the digital signature of the issuer. This certificate solely, the mobile node will communicate with each other. All nodes have their own private keys. The public and therefore the private keys are completely different. The public secret is used for encrypting the messages and also the personal key is used for cryptography to make sure authentication. The design of this technique is shown within the figure 1.

The Hybrid cryptographic algorithms comprise the following- Advanced Encryption Standard (AES) is employed to come up with the session key for sending the message. Rivest-Shamir-Adleman (RSA) is employed to come up with the general public and personal keys. Digital Signature Standard (DSS) is employed for the verification method and it uses Secure Hash Algorithm (SHA) to come up with hash price. This hash price is encrypted using public key of the recipient. This encrypted has value is employed for the verification method.

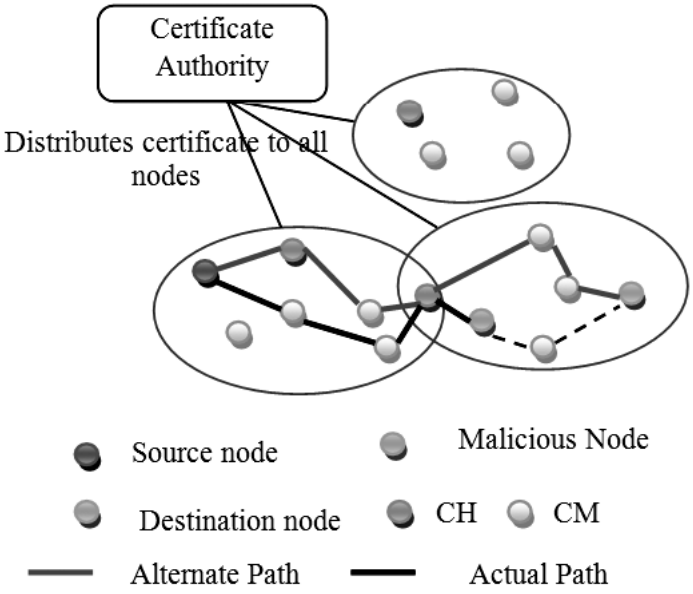

Figure 1: Proposed System Architecture

3.1. Secure Cluster Based Routing Using RNULVRP

To implement the transmission of messages from the source to the destination, it wants a shortest and stable path, since all the mobile nodes is also in moving state whereas transmittal the message. This will be through with the assistance of Restructured network based unclear logic Routing Protocol (RNULVRP) that is explained in further section. It reduces the routing connected overhead and discovers the shortest and stable path. This protocol finds the stable route supported the validation concept. Route construction ought to be through with a minimum of overhead and bandwidth consumption. It uses clustering's structure to decrease average end-to-end delay and improve the typical packet delivery ratio. Routing has two components- discovering the route and maintaining it supported metrics. Metrics embrace the expected transmission time, estimated transmission count, etc. If there is any malicious node within the path, alternate path is found.

3.1.1. Unstructured Network based unclear logic Routing

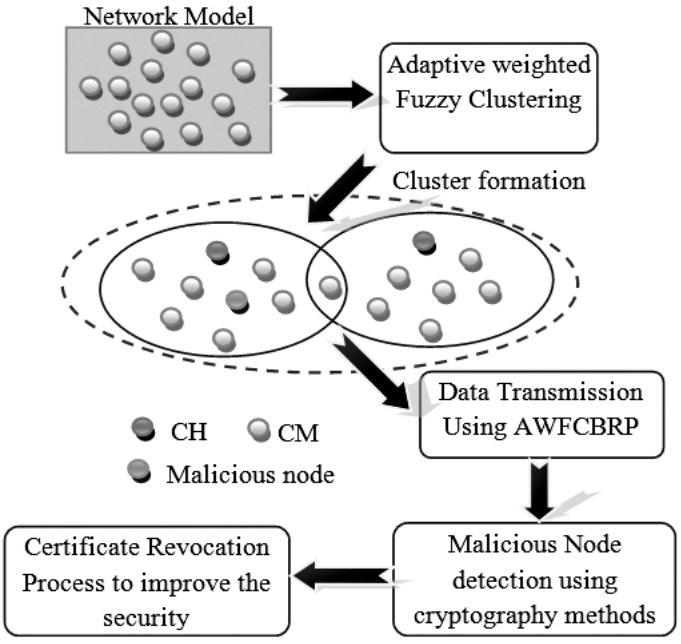

Figure 2: Proposed RNULVRP Architecture Diagram

This section discusses the planned for cluster head choosing, control protocols and routing for mobile ad-hoc networks very well. The design diagram is given in figure 2.

3.1.2. Cluster formation

At a specific time interval each node sends a beacon referred to as Alive Beacon (AB) where time stamp and NODE ID field are there in AB. the nodes that hear AB is checked with the neighbor data table (AT). AB sets it's AT field to zero and initiates a timer when there is a new entry is formed for the sender of AB once there is no entry with AB's NODE ID it creates a replacement entry for the sender of AB. Earlier to expiration of timer, if the NODE ID received in AB is same, it sets AT such as that node to one and restarts the timer. The corresponding entry within the NDT is removed. Abs isn't forwarded. Before the arrival of AB node if timer expire the subsequent node is taken into account to own moved and also the CH is wise to concerning this. Cluster head Beacon (CHBs) is detected by each node. There are four attainable cases:

1. The CH and also the node are within the cluster once a CHB is detected.
2. Once a node listens to one more cluster's CHB with its CHB, after that it inserts the CH ID of the former's CHB in an exceedingly Access table (AT). If at intervals a such amount of your time (GETTHRESHOLD) it hears each the CHBs all over again, it affirms itself because access among these two clusters then forwarding a "Access assert"(AA) packet to each the Hs. AT is checked by CH once it receives AA packet and appears for alternative gateway.

i) AA is affirmed of the absence of another gateway through storing the intermediate node ID in its GT and "access indexed" packet then.

ii) one time collect incorporates access entry the hop count of the present gateway is compared with the AA sender by the CH .When the hop count of the AA is a smaller amount than CH a "gateway indexed" packet is shipped to the AA when CH is deregistered. Otherwise AA packet is neglected. The AA packet is not sent for a specific amount of time and also the method is recurrent once more.

3. It register's with the cluster employing a "register me" packet once it hears the CHB of that cluster. The table of nodes that are accessible within the cluster of the CH is updated and a "registered packet" is shipped to the node.
4. If no CHB is detected two prospects happen

i) The node moves from the cluster. As delineated earlier the desired steps are taken once those nodes that have less hop count distance from the CH sight quality

ii) Once CH moves to a substantial distance the nodes begin the cluster formation part all over again by reversing for a random time interval.

3.1.3. Cluster Head Selection

Cluster heads are chosen based on the following weighted sum $W = w_1D_1 + w_2D_2 + w_3D_3$. Where D_1 is denotes the power intensity of the node, D_2 is the connectivity factor and D_2 is the stability index and finally, w_1, w_2 and w_3 are referred as the weighting factors where the cluster head has the least w value. Subsequent to the node is formed as a cluster head and the members of the node will be differentiated as "considered". Each "unconsidered" node undergoes the selection process. Afterward the selection of "considered nodes" the selection algorithm will be terminated.

Cluster Head Selection Algorithm

Begin CH_Selection ()

1. nodeweight=w1×E+w2×I
2. isclusterhead=1
3. maxweight=nodeweight
4. timer=1/nodeweight
5. if (timer<0)
6. CH_Announcment (nodeID, nodeweight)

Obtain Announcment (Sending Node ID, weight)

1. If (isclusterhead==1; ownweight<weight){
2. isclusterhead=0
3. Nodeclusterhead=SendingNodeID
4. maxweight=weight}
5. else if(isclusterhead==0){
6. If(maxweight<weight){
7. Nodeclusterhead=SendingNodeID
8. maxweight=weight}}

Send_Finalized_CH_Announcment()

1. If (isclusterhead==1)
2. Ultimate_CHAnnouncment(nodeID,nodeweight)
3. End

3.1.4. Intra-cluster Communication

In this, every normal node sends info to its cluster head. It is discovered throughout the simulations that the bulk of packet loss happens throughout intra-cluster communications once traditional nodes attempt to send info to their various cluster heads and thanks to node quality each cluster head moves remote from the transmission vary of traditional node or contrariwise. In this section, every cluster head collects info from its encompassing nodes that are related to that cluster head so sends the aggregative knowledge to the ultimate destination mentioned within the next section.

3.1.5. Inter-cluster Communication

In inter-cluster communication cluster head sends the aggregative data to their neighboring cluster heads. Throughout the simulations it is ascertained that in most cases two cluster heads don't seem to be at intervals transmission vary of every alternative. Therefore during this case they cannot send info to every alternative and it ends up in path breakage. As during inter cluster communication cluster heads sends the aggregative information of the whole round, therefore, just in case of path breakage if this info is lost, it will mean that the knowledge of the entire round is lost. So it is important for any routing protocol to use a recovery strategy. In RNULVRP, there is no recovery mechanism accessible and through simulations it had

been ascertained that the majority of the days, cluster heads were not ready to communicate with their neighboring cluster heads. In absence of any recovery mechanism, RNULVRP suffers heavily.

There are two approaches for recovery strategy. The primary one is hop-by-hop and also the second end-to-end. Hop-by-hop recovery is additional energy capable since retransmission remoteness is smaller. Contained by the planned work, use hop-by-hop recovery strategy driven from wireless broad cast advantage (WBA) that was planned. The fundamental mechanism in WBA is choice of guard nodes. WBA is predicated on the subsequent thought that as wireless transmissions are broadcast in nature, therefore, the neighboring nodes of the receiving node additionally receive the transmissions, and people neighboring nodes will get together to transmit that packet to the receiving node just in case of packet loss thanks to path breakage.

3.2. Authentication

To perform authentication, the CA acts just like the Authentication Controller and here it is accountable for distributing the certificate, generating session key. The authentication controller authenticates the supply before the transmission method starts. This method is applied as follows.

- Source gets the certificate from CA.
- Source sends the RREQ to destination.
- Destination requests the CA for session key to transmit the original message.
- CA verifies the identity of recipient and sends the session key to the destination.
- Destination sends the RREP to source.
- Currently the source starts sending the message.

After receiving the message, the receiver should check the integrity of the message, that is such because the authentication of message.

3.3. Malicious Node Identification

To spot the malicious node TWOACK [20] theme is employed. In line with this scheme, the destination should send the two hop acknowledgement to the sender for each and every packet at intervals a predefined amount of your time. If the acknowledgement is not received at intervals the required time which suggests this node either has not forwarded the packet to the neighborhood or it should discard the packet, the actual node is taken into account as a malicious node.

3.4. Certificate Revocation

When distinctive the malicious node within the path, its certificate ought to be revoked to isolate this malicious node from the network so it cannot ready to communicate with alternative nodes [21]. This improves the safety.

To revoke certificate of malicious node, the whole network is taken into account as a group of clusters. Every cluster has Cluster Head (CH), and a few Cluster Members (CMs). The node with high energy and additional packet handling capability is chosen as CH. The revocation method is performed as shown within the figure 3.

The steps within the revocation method are

- Neighbor node detects the attack and sends the accusation packet to CA through CH.
- CA revokes the certificate in line with the received packet.
- CA broadcasts the revocation message to all or any the nodes through CH.

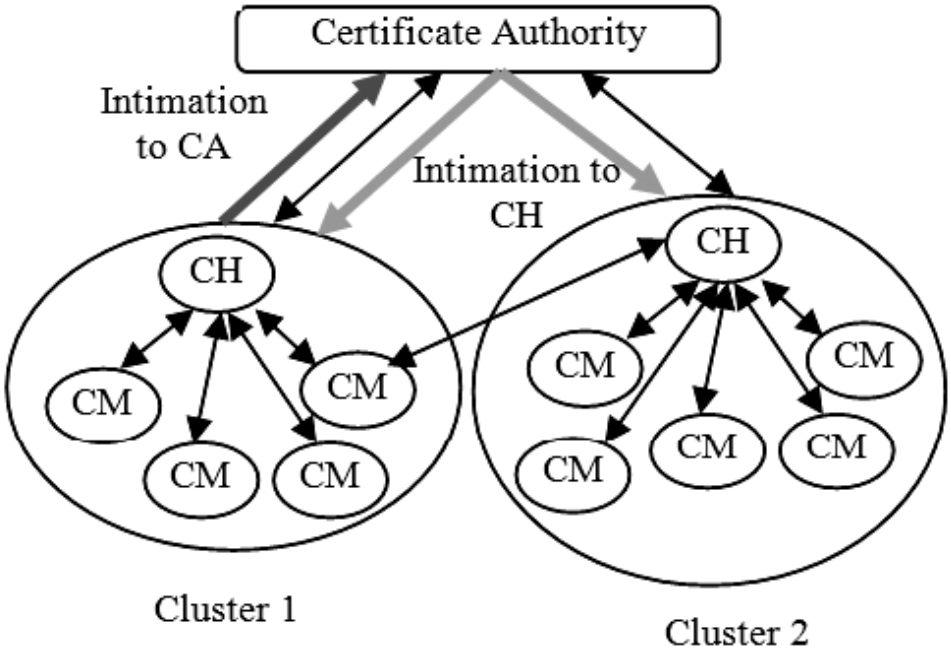

Figure 3: Certificate Revocation Process

3.5. False Accusation Identification

False accusation of an attacker node against the legitimate node degrades the strength and also the accuracy. To avoid this, the incorrectly suspect node ought to be known and rehabilitated at intervals its cluster. Since CH doesn't sight any attacks from the incorrectly suspect node, CH sends the recovery packet to CA. Using this, CA restores this node.

The steps during this method are

- CH sends the recovery packet to CA.
- CA restores the certificate of the incorrectly suspect node.
- The incorrectly suspect node is currently rehabilitated within the cluster so it will communicate with alternative nodes.

4. EXPERIMENTAL RESULTS AND DISCUSSION

Initially, authentication and therefore the public and private key generation are distributed at the initial stage. Subsequently, the certificate revocation of the malicious node is completed. At long last, if there is any incorrectly suspect node, it is fixed. The virtual implementation of the entire process is deployed by means of Network simulator (NS 2.34) and run in Linux OS. The MANET environment is built with 50 mobile nodes and that they move with a speed of 1 to 10 m/s. The transmission range is mounted as 250m. The malicious node launches attack each 5 seconds. The nodes are deployed in an exceedingly uniform random distribution. The performance of the projected technique is differentiated with existing schemes such NCPR [22], and CLMNRP [23].

4.1. Network Lifetime

Figure 4 denotes network lifetime vs. number of nodes. Network lifetime is estimated based on nodes get energetic in how long process will continue. In simulation report existing work NCPR and CLMNRP network lifespan is a lesser as compared to RNULVRP proposed work. Since network nodes are active to continue communication in maximum time.

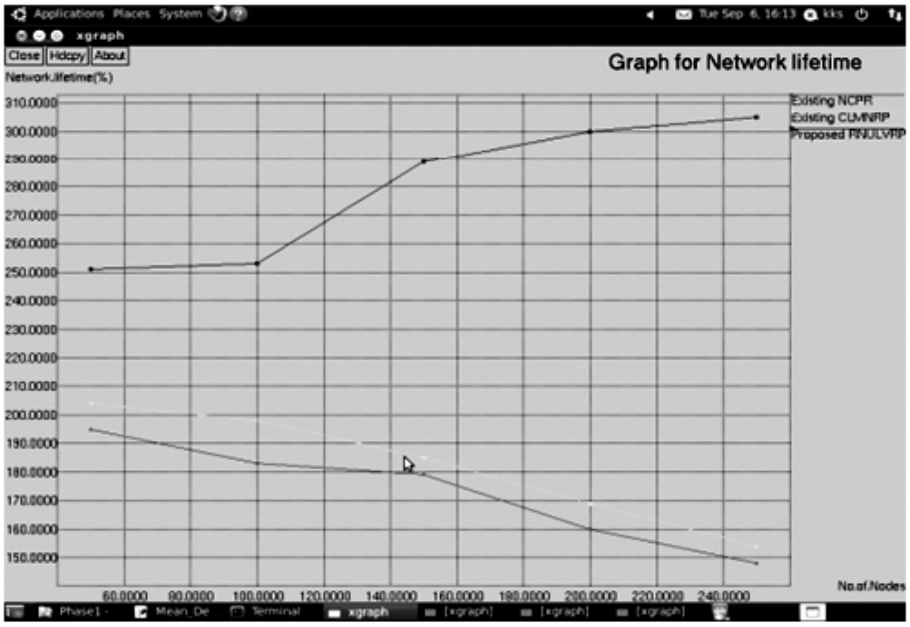

Figure 4: Number of nodes vs. Network life time

4.2. Packet Loss

In Figure 5 shows the transmission of packets which are dropped with different speed of nodes in network. In simulation output the velocity improves packets are dropped also improved. In existing CBRP with SBCA does not have any recovery mechanisms the numbers of packets that are lost are on the maximum aspect. The previous methods NCPR and CLMNRP maximum as compared to the present RNULVRP contains a recovery scheme, it reduces the packet loss.

4.3. Mean Delay

Figure 6 denotes number of nodes vs. mean delay. Simulation report shows node count will increase the mean delay also get increases in any technique. The proposed RNULVRP is analyzed to create minimum mean delay when compared with the existing routing schemes such as NCPR and CLMNRP.

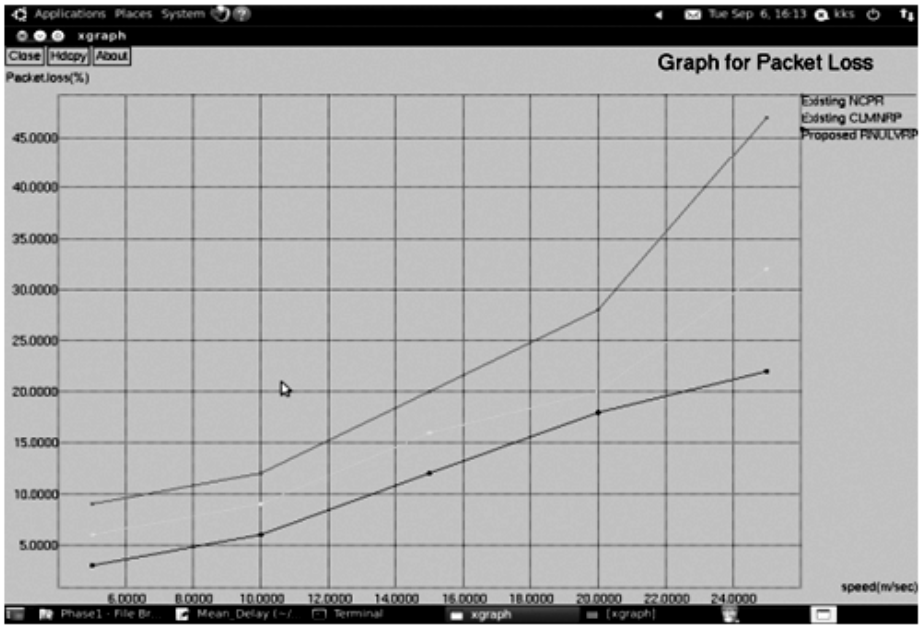

Figure 5: speed vs. Packet loss

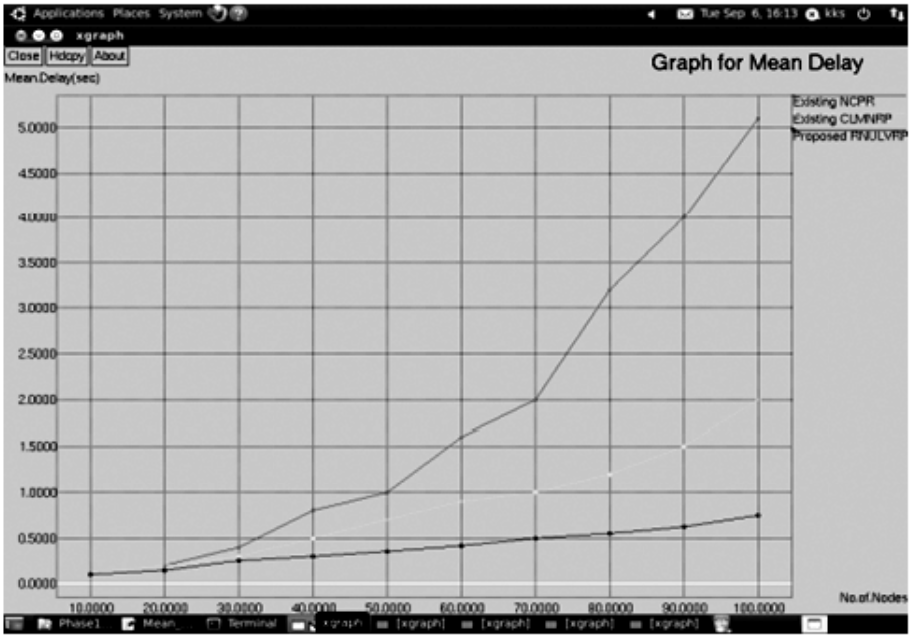

Figure 6: Number of node vs. Mean delay

4.4. Throughput

In Figure 7 shows throughput. Proposed RNULVRP approach to reorganize the path during broadcasting of data packets to achieve maximum throughput when compared with the previous methods are NCPR and CLMNRP in each communication.

4.5. Packet Delivery Ratio

The Figure 8 shows packet delivery ratio vs. various speed. Simulation results show the speed will improve, the packet delivery ratio decreases in each techniques. RNULVRP report different two protocols in terms of packet delivery ratio. It has been exposed that using WBA as the recovery scheme to enhance packet delivery ratio compared with NCPR and CLMNRP existing methods.

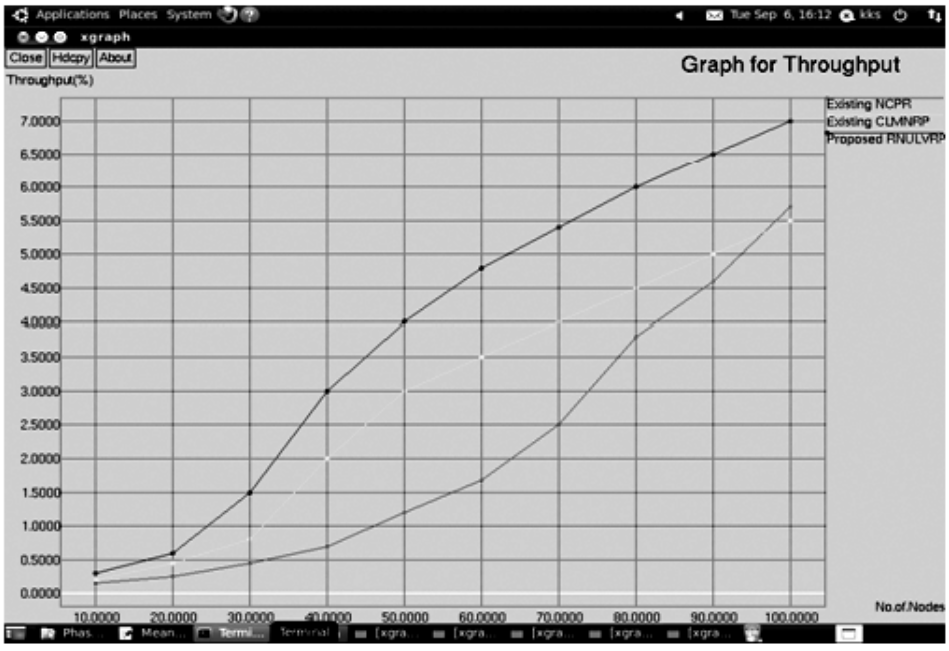

Figure 7: Number of node vs. Throughput

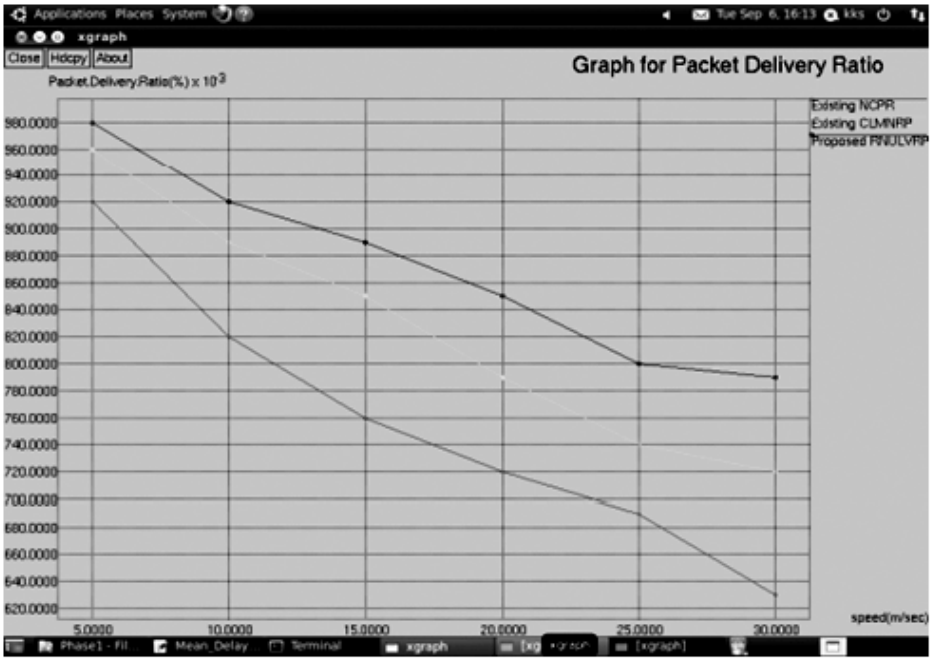

Figure 8: speed vs. Packet Delivery ratio

5. CONCLUSION

Mobile nodes are get grouped to perform process decide the link issues. In Proposed RNULVRP approach, that efficient to finding out the malicious node and revokes the certificate with less time and resource. If there is any incorrectly accused node, its certificate is revoked. This improves the performance, accuracy, and dependability of the network. Clusters are formed to create the revocation method faster, that reduces the network traffic. The effectiveness of the cluster based mostly technique has been experimented mistreatment network simulator. The future research is centered on a lot of efficient and effective clustering schemes and a mix of various parameters in selecting the effective Cluster Head in Cluster Topology for MANET.

REFERENCES

[1] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N. Kato, "A Survey of Routing Attacks in MANET," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[2] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, June 2009.

[3] P. Sakarindr and N. Ansari, "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," IEEE Wireless Comm., vol. 14, no. 5, pp. 8-20, Oct. 2007.

[4] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions,"IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[5] P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks"IEEE Wireless Communications, vol.14, no. 5, pp. 8-20, 2007.

[6] S. Micali, "Efficient certificate revocation," Massachusetts institute of technology, Cambridge, MA, 1996.

[7] 13. K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate revocation to cope with false accusations in mobile ad hoc networks," in Proc. 2010 IEEE 71st Vehicular Technology Conference: VTC2010-Spring, Taipei, Taiwan , May 16-19, 2010.

[8] GSR Emil Selvan, Dr. M. Suganthi, P Jeni, KA Krishna Priya, "Detection of Compromised Nodes in Mobile Ad-Hoc Networks", Journal of Computational Information Systems, pp 1823-1829, 2011.

[9] S.M. Sarwarul Islam Rizvi, Zinat Sultana, Bo Sun, Md. Washiqul Islam, "Security of Mobile Agent in Ad hoc Network using Threshold Cryptography", World Academy of Science, Engineering and Technology, 2010.

[10] Sanjay Raghani, Durga Toshniwal, R. C. Joshi, "Distributed Certification Authority for Mobile Ad Hoc Networks – A Dynamic Approach", Journal of Convergence Information Technology, Volume 2, Number 2, June 2007.

[11] Keun-Ho Lee, Sang-Bum Han, Heyi-Sook Suh, "Authentication Protocol Using Threshold Certification in Hierarchical-cluster-based Ad Hoc Networks", Journal of information science and engineering, pp 539-567, 2007.

[12] 10. M. Jiang, J. Ji, Y.C. Tay, "Cluster based routing protocol, Internet Draft", draft-ietf-manet-cbrp-spec-01 .txt, work in progress, 1999.

[13] Mehran Abolhasan, Tadeusz Wysocki and Eryk Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," 2003 Elsevier

[14] Mohamed Dyabi and Hakim Allali "A new MANETs clustering algorithm based on nodes performances" Fifth International Conference on Next Generation Networks and Services (NGNS), IEEE, May 28-30, 2014.

[15] Mike Burmester, Breno de Medeiros "On the Security of Route Discovery in MANETs" IEEE transaction on mobile computing, p.p. 1- 9, 2011.

[16] Subbian Umamaheswari and Govindaraju Radhamani "Enhanced ANTSEC Framework with Cluster based Cooperative Caching in Mobile Ad Hoc Networks " Journal of Communications and Networks, IEEE 1, February 2015

[17] Soumyabrata Talapatra and Alak Roy "Mobility based Cluster head selection algorithm for mobile ad-hoc Network" I.J. Computer Network and Information Security, p.p. 42-49, June 2014.

[18] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, Karl Levitt "A specification based Intrusion detection System for AODV" Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, Oct- 2003.

[19] Minakshi and Rakesh Gill "Secure AODV using HMAC-MD6 in MANET" IJCSMS International Journal of computer science and management Studies, Vol. 13, Issue 09, p.p. 16-23, Nov- 2013.

[20] K.Liu,J.Deng, P.K.Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[21] Wei Liu,Hiroki Nishiyama,Nirwan Ansari,Jie Yang,Nei Kato,"Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks",IEEE Transactions On Parallel And Distributed Systems,Vol.24,No.2, February 2013.

[22] Zhang, X.M., Wang, E.B., Xia, J.J. and Sung, D.K., 2013. A neighbor coverage-based probabilistic rebroadcast for reducing routing overhead in mobile ad hoc networks. IEEE Transactions on Mobile Computing, 12(3), pp.424-433.

[23] Rajaram, A., And Shajan Joseph. "Cluster Based Neighbor Coverage Routing Scheme For MANET." Journal of Theoretical & Applied Information Technology 68, no. 3 (2014).