I J C T A, 10(20), 2017, pp. 25-39 ISSN: 0974-5572

A Novel Enhanced SVM Cluster Based Secure and Effective Routing Protocol for Node Authentication in Mobile AD HOC Networks

Shajan Joseph* and A. Rajaram**

ABSTRACT

MANET is an autonomous organization of mobile nodes which are unengaged to move and organize themselves and alter topology dynamically, establishing a best and economical route between the communicating parties is that the primary concern of the routing protocols of painter. However one amongst the most challenges in MANET is to design the strong security resolution which will defend MANET from many routing intruders. Totally various schemes are projected to countermeasure the routing attacks against mobile network. So, preventing and detecting the malicious nodes from destroying the network plays important role in ad hoc networks. During this work, a completely unique technique has been projected to create node authentication whereas a new node adhering into the network and earlier than initiating route discovery method in mobile ad hoc networks. Initially, a completely unique enhanced Support Vector Machine (ESVM) clustering algorithm is employed to dynamically cluster nodes in MANETs into logically separating or non-overlapping entities, referred to as clusters. Afterwards, a unique node authentication technique is projected for MANETs which will be simply integrated with the projected routing protocol and provides security. Based on the simulation results, the projected enhanced SVM Cluster based Secure and Effective Routing Protocol (ESVM-CBSERP) achieves higher performance than previous protocols based on the parameters such as packet reliability rate, mean delay, end to end delay, throughput, network lifetime etc.

Keywords: MANET, Security, Enhanced SVM Clustering, Node Authentication technique**.**

1. INTRODUCTION

Mobile Ad hoc Network may be a set of wireless mobile nodes that cooperatively form a network while not explicit organization or design. This is a special kind of wireless network by that the mobile hosts are connected by wireless interfaces to create a brief network with none mounted infrastructure. In MANET, nodes communicate one another by forming a multi-hop radio network. In multi-hop network scenario, success of the communication depends on node's cooperation [1]. Since nodes could exhibit totally different mobility behaviors, the topology of the network is unpredictable and changes often [2, 3].

The application of MANET includes military battlefields, emergency search, and rescue locations etc. That needs fast preparation and active re-configuration. The most constraints for MANET are restricted bandwidth and restricted battery power [4]. A basic vulnerability of MANET comes from open peer to look design. Not like wired networks that have dedicated routers, every mobile node in a very MANET could operate as router and forwards packets to different nodes. On the opposite hand, wireless channel is accessible to each legitimate network users and malicious attackers. As a result, there's no clear line of defense in MANETs from the security design perspective.

* 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*

The salient options of MANET cause each challenges and opportunities in achieving the higher than security goals [5]. First, use of wireless links render status to link attacks starting from passive eavesdropping to active some process like impersonation, message rerun and message deformation. The nodes roaming in hostile surroundings with comparatively underprivileged protection have non negligible chance of being compromised. Therefore, we should always not solely contemplate malicious attacks from outside a network. However conjointly take under consideration the attacks launched from inside the network by compromised nodes [6].

Therefore to realize high survivability, mantes ought to have a distributed design with no central entities. MANET is additionally dynamic, as a result of frequent changes in each its topology and its membership. Trust relationship among nodes conjointly changes; as a result of a brand new node could be part of or leave which node could also be compromised. Finally a MANET could contain tons of or maybe thousands of nodes. Security mechanisms ought to be ascendable to handle such massive networks.

With this motivation, during this work an increased SVM Cluster based mostly Secure and Effective Routing Protocol (ESVM-CBSERP) based on the energy is planned. Hereby preventing the malicious nodes from destroying the network plays important role in unexpected networks. During this work, a unique technique has been planned to give node authentication whereas a new node joining into the network and before initiating route discovery method in mobile unexpected networks. The remains of the paper are planned as follows. In part 2, the literature study is specified. In proposed ESVM-CBSERP workings are denoted in Part 3. In part 4, it offers the comparison of the projected protocols with the utilization of simulation results. Finally, part 5 describes the conclusions and future scope.

2. BACKGROUND STUDY

In [7] the author projected efficient Position based opportunistic protocol supported stateless geographic routing property and broadcast nature. This protocol offers with virtual destination based mostly void handling to avoid the communication holes. Just in case of link breakage, choosing forwarding nodes were specified.

Slim et al. [8] have projected the protection problems to be addressed in routing protocols outlined within the scope of aeronautical ad hoc networks. Existing routing approaches are shortly mentioned, so a secure geographical routing protocol for future craft circumstantial networks is projected. Finally the protocol is formally verified and its performances are mentioned.

In [9] the nodes that have the upper trust worth is taken into account because the best forwarder. The self-seeking and traditional node is differentiated by the use of the RREQ algorithm. The egoistic nodes don't forward the request. It will check the trust worth, whether or not it is stronger or acquaintances. Although they use RREQ algorithm exploitation proactive routing technique is not ascendable and maintenance of routing table needs substantial network resources.

In POR the most effective forwarder is not checked whether or not it is secured or not. Encryption, integrity, Identity and site privacy is not handled. Leimuller et al. [10] have projected a detection mechanism that's capable of recognizing nodes cheating regarding their position in beacons (periodic position dissemination in most single-path geographic routing protocols, e.g. GPSR).

In the previous work [11], optimized multicast routing scheme has been introduced to achieve additional network stability. During this work, the estimation of link stability, path stability and node stability is set to produce additional network stability. The trustable network was shaped supported stability model.

In [12], authors conferred a performance analysis of an increased version of the Topological Multicast Routing algorithm (ToMuRo). It enclosed undecided border nodes. The undecided border nodes were accustomed forward multicast packets to optimize the trail discovery method. It had been done by selecting

undecided nodes that may operate as multicast relay nodes. However during this work, there was no stable and reliable model increased to support optimum routing packet delivery.

In [13], authors thought of routes length with its route choice method which includes routes energy in its calculations. It developed the routing issue as an optimisation downside so used Binary Particle Swarm optimisation algorithmic rule to decide on a route that maximizes a weighted operate of the route length and also the route energy.

Shen and Zhao [14] present an ALERT-Anonymous Location-based economical Routing protocol. Energetically splits the network field into parts and that chance to selects nodes in parts as intermediate neighbor nodes, in that type no traceable unidentified path. Consequently, ALERT offer namelessness security to sender, receiver, and intermediate nodes. Moreover have schemes to successfully counter connection and secular order intruders. Furthermore, ALERT obtains comparable communicating strength to the GPSR environmental communication scheme. except it is at danger of choice of intruders.

EI Defrawy et al. [15] have projected some fascinating problems arising in such MANETs by coming up with an anonymous routing framework (ALARM). It uses nodes current locations to construct a secure MANET map. Supported this map, every node will decide that alternative nodes it needs to speak with. ALARM takes advantage of some advanced science primitives to realize node authentication, information integrity, namelessness and untraceability (tracking-resistance). It additionally offers resistance to bound corporate executive attacks.

Lyu et al. [16] have projected economical and Secure Geographic Routing protocol (ESGR) that utilizes the geographic leashes and also the TESLA theme to produce resistance against Sybil attacks. Additionally to the present, it utilizes a distributed trust model and opportunistic packet forwarding method to forestall region and grey hole attacks.

Zhang et al. [17] have projected a cross-layer distributed algorithmic rule referred to as interference-based topology control algorithmic rule for delay-constrained (ITCD) MANETs with considering each the interference constraint and also the delay constraint (IBTC) that involves high process and storage overhead. A biological model of physarum [18, 19] is employed for coming up with novel biology-inspired optimisation algorithmic rule for minimal exposure problem (MEP). It converts MEP into the Steiner downside by considering the observation field into a large-scale weighted grid.

3. PROPOSED METHODOLGY

We assume that there are mobile nodes roaming in a $R \times R$ km sq., and every move consistent with the RRGM (Reference Region cluster mobility Model) [20]. All nodes have same transmission vary of r Km ($r<R$). Every node will acquire their position and time information through GPS and may additionally broadcast them to their neighbors. The improved Support Vector Machine (ESVM) clustering algorithm is employed for the agglomeration low-level formatting and accustomed chooses the cluster head that is delineated below intimately.

3.1. Cluster initialization

Prior to the cluster initialization, all nodes are within the state of NULL. Once started, every node within the network broadcasts a HELLO message to own information of its member nodes. Then, every node broadcasts a CH_SELECT message to its neighbor. Upon receiving, it'll compare the value metric with itself, and also the larger one is elective as a cluster head. Finally, the cluster head can broadcast the elective ensuing message referred to as CH_CLAIM (cluster head claim) to its one-hop neighbors.

Upon receiving, the neighbors can send RTJ (Request To Join) message to the cluster head, and cluster head can send ATJ (Affirm To Join) back once agreeing. Once the on top of method, some clusters can are

fashioned. However once a cluster member receives over one ATJ message, this denotes that the node lies in separate clusters however among transmission vary of one another; so it will be elective as a gateway between these clusters.

Once the initial clustering phrase takes place, cluster heads and cluster members should exchange message to keep up the link sporadically. Namely, the cluster head sporadically broadcasts CH_CLAIM (cluster ID) messages to its neighboring nodes. And also the cluster members of the hooked up cluster broadcast cluster member (node ID, cluster ids) messages back to the cluster head sporadically, wherever the node ID is that the symbol of the broadcasting node, and cluster ID is that the list of clusters of that the node could be a member.

(1) Deleting or Adding Nodes. If the node doesn't hear periodic broadcast from its cluster head then the cluster member would dissociate from the hooked up cluster. Also, the cluster head can take away the cluster member from its list of members, if it doesn't receive the periodic cluster member broadcasts.

When a node, as well as new returning or unconnected from different clusters, needs to hitch a cluster, it ought to send RTJ to a cluster head, and also the cluster head can send a ATJ message back given that the requesting node is allowed to hitch.

Note that once a node moves out of its cluster head' transmission vary however still incorporates a link to a different cluster member happiness to any cluster head, it'll become a cluster guest to avoid a brand new initial clustering formation going down, although the cluster guest's value metric is larger or not. During this manner, it will scale back the cluster head amendment rate, and also the ripple effects caused by reclustering will be unheeded. Therefore the routing overhead is dried-up.

(2) Substitution the Cluster Head Position. Once a cluster head leaves its own cluster or is broken, the node happiness to the current cluster would come back to the NULL state. Thus, they ought to request connection different clusters or establish a new cluster. Note that only if the node receives over two consecutive RTJ messages from another bound node, ought to they establish a brand new cluster.

(3) Merging completely different two Clusters. Once a cluster enters the transmission vary of another cluster and also the variance of value metric of the two cluster heads is tiny, that denotes that the two clusters are worth merging. If so, the cluster head that has larger metric are reelected because the new cluster head, however the similar one should quit its cluster head role to be a typical member of the new cluster. Otherwise, it denotes that the two clusters simply incidentally move one another in a very short amount and it is disgraceful of merging. During this manner, it will scale back the chance of cluster overlapping.

3.2. ESVM Clustering

An SVM-based clustering algorithm is a new clustering method which is established the clusters knowledge with no a priori information of input classes. Once this low-level formatting step is complete, the SVM confidence parameters for classification on every of the coaching instances will be accessed. All-time low confidence knowledge then has its' labels switched to the opposite class label. The SVM is then re-run on the network and is absolute to converge during this state of affairs since it converged antecedently, and currently its fewer knowledge points to hold with mislabelling penalties. This approach seems to limit exposure to the native minima traps that may occur with different approaches. Thus, the rule then improves on it's debile convergent result by SVM re-training once every re-labeling on the worst of the misclassified vectors – i.e., those feature vectors confidently issue values on the far side some threshold. The repetition is higher than the other methods which improve the accuracy, here a live of disconnectedness, till there aren't any misclassifications.

The network region is linearly dissociable, linear ESVM computes the utmost margin linear classifier. The SVM clustering case is an extension that enables effective clustering of comparable mobile nodes

inside the transmission vary. The ESVM approach cope with multi labeled of conception with 'm' categories and it decompose the problem into 'm' binary issues. There exist recent decomposition strategies that appear to be additional dominant. However, for ease and for distinction with associated results select straightforward decomposition for ESVM grouping.

Initially hello-concept hyper plane is made by the clustering rule with one set of points corresponds to the set of nodes' messages, and also the different corresponds to the sets of extracted regions. The boundary hyperplanes on the two categories of nodes are separated by a distance 2/w, called the "margin" where $w^2 = w_\beta w_\beta$. Through escalating the margin between the separated nodes so far as possible the SVM's optimal separating hyperplane is attained. In the standard SVM formulation, the objective to maximize w^{-1} is reaffirmed as the goal to reduce w^2. The augmented Lagrangian formulation subsequently chooses an optimum described at a saddle point of

$$L_A\left(x, y, w, b, \alpha\right) = \left(\frac{W_\beta}{2}\right) - \alpha_\gamma y_{\gamma\beta} - \left(w_\beta x_{\gamma\beta} - \times b\right)$$

$$-\alpha$$

In theory, the positive parameter w_β in the augmented Lagrangian function, recognized as the penalty parameter that can also be changed from iteration to iteration, where $\alpha = \sum\gamma\, \alpha_\gamma\, \alpha_\gamma > 0$ $(1 \le \gamma \le M)$. The saddle point is obtained by minimizing with respect to $\{w_1, ..., w_N, b\}$ and maximizing with respect to $\{a_1, ..., a_M\}$. Let $\{x_i\}$ be an extorted concepts of N nodes in a space. Similar to the nonlinear SVM formulation, by means of a non-linear transformation, transform x to a high-dimensional space referred as Kernel space and look for the smallest enclosing sphere of radius R. The mahalanobis distance formula for similarity matching is given as follows

$$\left\| \sqrt{\phi\left(x_j\right)^2 - a} \right\| \le R^2 \quad \text{For all } j = 1, ..., N$$

Where a is the center of the sphere, from the center point the clusters are formed based on the ||.|| Mahalanobis distance. Currently, the cluster assignment is determined as follows. Let a segment of nodes y, the clustering rule can be symbolized as the adjacency matrix is known as follows

$$A_{ij} = \begin{cases} \forall y & \textit{on the line segment connecting } x_i \textit{ and } x_j \\ 0 & \textit{otherwise} \end{cases}$$

All mobile nodes area unit checked to assign a particular cluster. The ESVM clustering rule iteratively merges the foremost similar try of nodes. Rule one shows the small print of ESVM the agglomeration rule, a hello message is made among all nodes as input for the clustering rule. To implement this, we tend to divide clustering into two steps. Within the initial clustering step, ESVM is used to cluster all the nodes, however it'd not merge identical transmission vary of nodes from completely different areas. Once getting all the clusters from the initial clustering step, the community merging step is used to merge node clusters containing identical energies from completely different nodes.

Algorithm 1: mSVM Clustering Algorithm for Query Cluster and profile management process

Input: Number of Nodes N, Energy of node

Output: Clustering of $\{N\}$, A Clustered network model

// Initial Clustering

Initialize mobie nodes $\{N\}$

Apply ESVM for clustering $Cl(A, B)$

Cl_A := {non-bounded support vectors of A},

If (Cl_A contains more elements than R)

then R : = Cl_A.

SV_A := {the support vectors of class A},

A : A minus SV_A,

$SV\_B := SV\_A$

//Build clusters portions

Let $R = \{r_1, ..., r_k\}$(obtained from Step 2).

$Cl := \{Cl_1, ..., Cl_k\}$

With

$Cl_i\{x \text{ in } X \text{ closer to } r_i \text{ than to any other } r_j\}$

// Join clusters portions

Repeat the following statement until Cl does not change.

for each $Cl_i \in Cl$:

c_i := Adjacency matix of Cl_i,

Find Cl_j containing a point closest to c_i using mahalanobis distance metric

$Cl\{x_i\} := (Cl - \{Cl_i, Cl_j\}) \cup \{Cl_i, Cl_j\}$,

If (score $Cl\{x_i\}$< score(Cl))

then Cl:= $Cl\{x_i\}$.

// Community Merging

Step 6. Obtain the similarity scores $Cl\{x_i\}$ for all possible energies of nodes using mahalanobis distance correlation.

Step 7. Merge the pair of most similar energies nodes (E_i, E_j) that contains the same energies from different nodes.

Step 8. Unless termination is reached, repeat steps 6 and 7.

3.3. ESVM Clustering Routing Protocol

In order to utilize the network resources with efficiency, ESVM clustering routing protocol is employed to proactive strategy between nodes at intervals individual clusters and reactive strategy between clusters, not like CBRP to use on-demand strategy between nodes of each intracluster and intercluster communication to strictly decrease the routing overhead and HSR, CGSR to use table-driven strategy to communicate in each intra- and interzone to decrease average end-to-end delay however increase the price of routing overhead unwillingly. In ESVM clump routing protocol, unless necessary, it will not activate the routing update method as so much as doable to avoid extra expenses in each intracluster and intercluster communication and route maintenance phrase. The packet format is shown in Fig.1.

3.4. Intracluster Communication

If the source and destination are within the same cluster, the information packet may be transmitted directly or relayed by cluster head. Namely, once the destination is within the range of source, source and destination will communicate with one another directly or relayed by cluster head. Otherwise, source and destination should exchange knowledge through cluster head.

Source node ID	Source node IP	Residual energy	Destination node IP	Destination node ID

Figure1: Packet Format

3.5. Intercluster Communication

If the source and destination are within the completely different clusters, the source should take the intracluster strategy. Namely, at first, the source sends a RREQ message to its hooked up cluster head then the cluster head can broadcast this RREQ to its adjacent cluster head through entranceway nodes, and therefore the method can continue till the RREQ arrives at the cluster that belongs to the destination node. Finally, the cluster head as well as the destination sends a RREP message back on the discovered path. Note that the cluster head within the discovered path can transfer the RREP on the native shortest route. Thus, the source can get the shortest route to the destination.

3.6. Route Maintenance

Due to the frequent topology detection, an efficient and effective technique of route maintenance in response to underlying topology modification is imperative as a result of while not routes validity the performance of a routing theme during a dynamic, mobile setting is affected even adversely.

When an existing link is failure (such because the node on the existing path that moves out of its one-hop neighbor or exits from the network or the receiving node on the present path cannot receive message from causing node owing to deterioration of the channel), the native repairing method would occur. Namely, an existing shorter path can replace the first route between the two nodes at that link is broken. Meanwhile, transparent messages are forwarded to the source node that originates the packets to advise the modification.

Note that, so as to make sure the validity and stability of route, the native repairing method will occur, only the intercluster routes are nullified. And this mechanism is extremely useful to scale back the route reestablishing expenses and end-to-end delay. The proposed work is shown in Figure 2.

3.7. Novel Node Authentication Technique For Preventing And Detecting Malicious Node

To provide secure routing preventing malicious node in MANETs, authentication of nodes by the network is to be in hot water the management packets; that's, the nodes receiving asking or reply packet should demonstrate the leader sent it. The mechanism for providing authentication ought to impose of tiny computations as a result of the very fact that MANETs square measure with restricted resources. The planned mechanism uses ones compliment and RSA algorithmic rule to produce security in routing.

In the proposed mechanism, authentication is enforced at two steps. At first each node on the network before causing a RREQ, it is needed to append ones compliment of its own node ip address and conceiver signs the destination node ip address with public key second. The receiving node checks the packet authentication of its source by adding the appended ones compliment and source ip address to that to urge all ones however the encrypted text cannot be decrypted. Any node concealed into the network not responsive to appending ones compliment of its ip address, the packets kind such nodes can get born by its neighbours. At an equivalent time if a node fails authentication, a warning message is broadcasted over the network, indicating the presence of a malicious nodes beside its scientific discipline address. Saving the time interval of different neighbor nodes receiving packets from the malicious node, simply by discarding them with none additional verification creating malicious node isolated on the network. On receiving of RREQ by the destination node, it decrypts with the personal key and integrity of source and destination ip address is checked. Just in case if destination finds any altered transmission it raises a warning over the network, else RREP packet is generated and sent to the source. The source verifies the authentication of destination on receiving RREP.

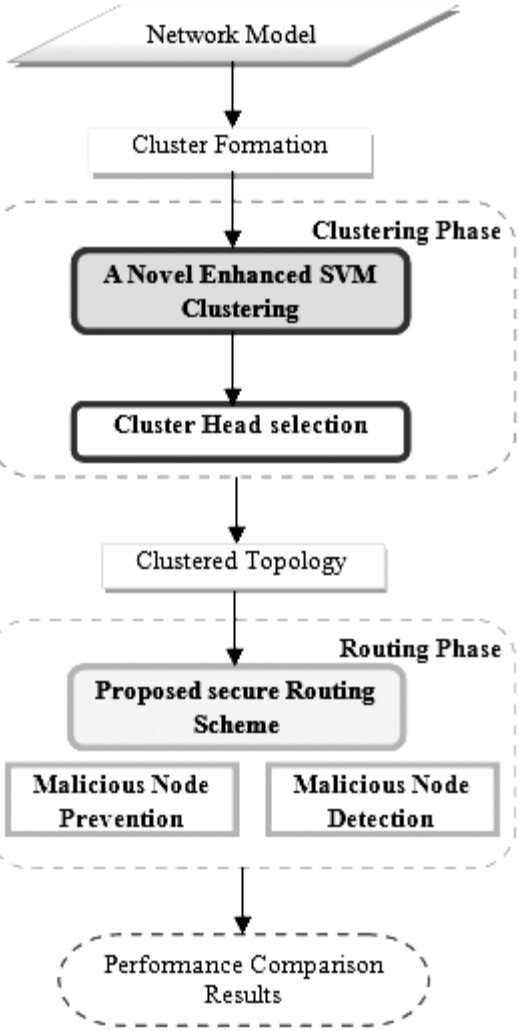
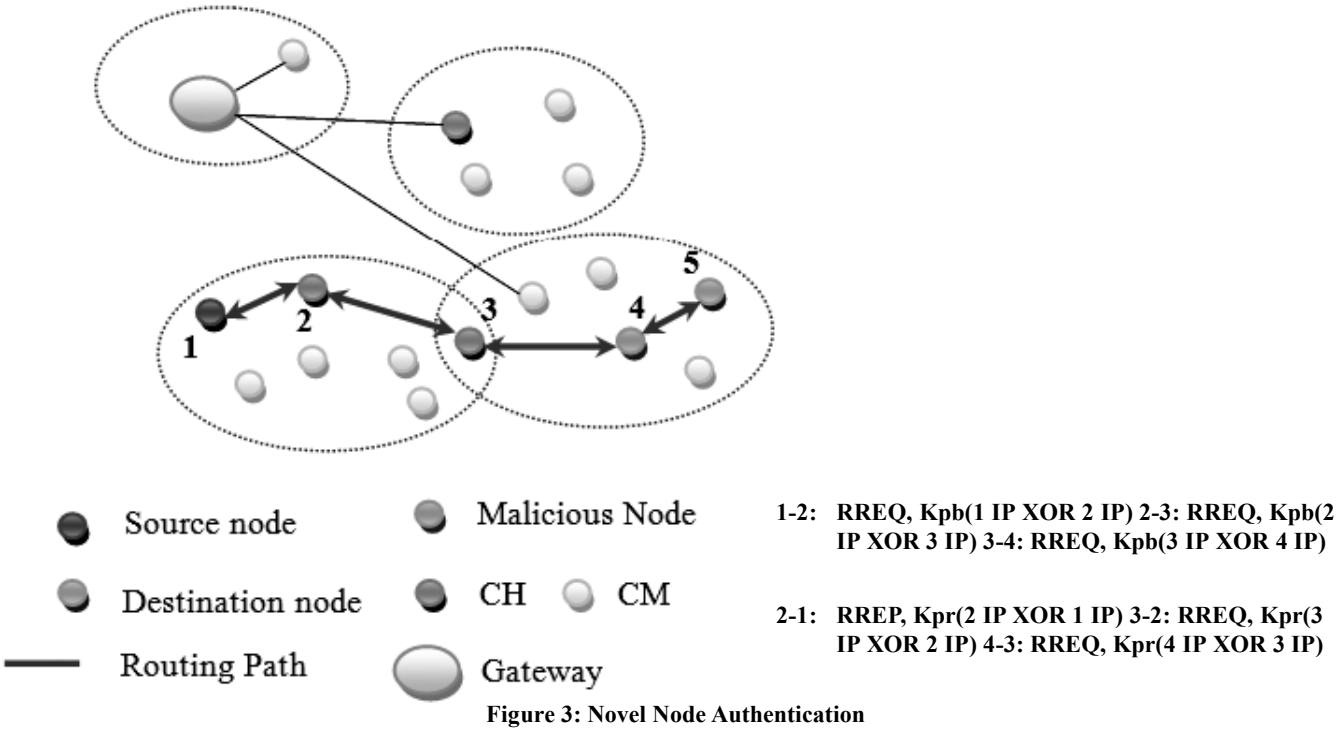


Figure 2: Architecture Diagram for ESFCRP



1-2: RREQ, Kpb(1 IP XOR 2 IP) 2-3: RREQ, Kpb(2 IP XOR 3 IP) 3-4: RREQ, Kpb(3 IP XOR 4 IP)

2-1: RREP, Kpr(2 IP XOR 1 IP) 3-2: RREQ, Kpr(3 IP XOR 2 IP) 4-3: RREQ, Kpr(4 IP XOR 3 IP)

Figure 3: Novel Node Authentication

Novel Node Authentication Technique Algorithm

1. Initially 1's complement of node's IP address is found
2. 1 IP XOR 5 IP = x
3. Node 1 sends RREQ encrypting x with public key, K_{pb}
4. Encrypted RREQ is sent to neighbouring nodes
5. On receiving RREQ, neighbouring nodes verify IP by appending 1s complement and forwards to destination
6. In the process of transmission, every node receiving verifies RREQ, but will not be able to decrypt the cipher text and forwards to the next node
7. Similarly every node does the same
8. Finally RREQ is received at 5 and decrypts the cipher text with the private key, K_{pr}
9. $x = C_e(\text{mod } n)$ gives plain text
10. (x XOR D IP) gives 1 IP, verification of IPs is done as in RREQ
11. If the IPs matched, node 5 encrypts RREP and transmits to source node 1, else a warning is sent to the neighbouring nodes over the network.

4. EXPERIMENTAL RESULTS AND DISCUSSION

This part the characteristics of proposed ESVM-CBSERP are estimated in NS-2.34 network simulator. The Output of ESVM-CBSERP scheme removes the intruder during transmission period. The results and observations of the proposed Enhanced SVM Cluster Based Secure and Effective Routing Protocol (ESVM-CBSERP) along with preceding protocols such as ESFCRP -Efficient Secure and Fair Cluster Routing Protocol, NCPR-Neighbor Coverage-Based Probabilistic Rebroadcast Protocol, and as well the CLMNRP and AWFCBRP in analyze various parameters.

4.1. Packet Delivery Ratio

In Figure 4 denotes packet delivery ratio vs. node speeds. The proposed ESVM-CBSERP increase its packet delivery ratio compared to Existing schemes is NCPR, CLMNRP, AWFCBRP and ESFCRP. In proposed work ESVM-CBSERP minimizes the probability of retransmission and minimizes the packet latency for all packet transmission, finally packet delivery ratio is improved.

4.2. Packet Loss

Figure 5 indicates the packets loss vs. node speeds. Diagram indicates speed will raise the quantity of packets losses also will raise. The present ESVM-CBSERP includes protection technique, amount of packet get losses is a minimum as compared to existing methods are NCPR, AWFCBRP, ESFCRP, and CLMNRP.

4.3. Network Lifetime

Figure 6 shows evaluation of Network Lifetime. In present work easy to find attacks before starts packet transmission. In existing schemes are NCPR, ESFCRP, AWFCBRP, and CLMNRP the network lifetime is minimum as compared to ESVM-CBSERP.

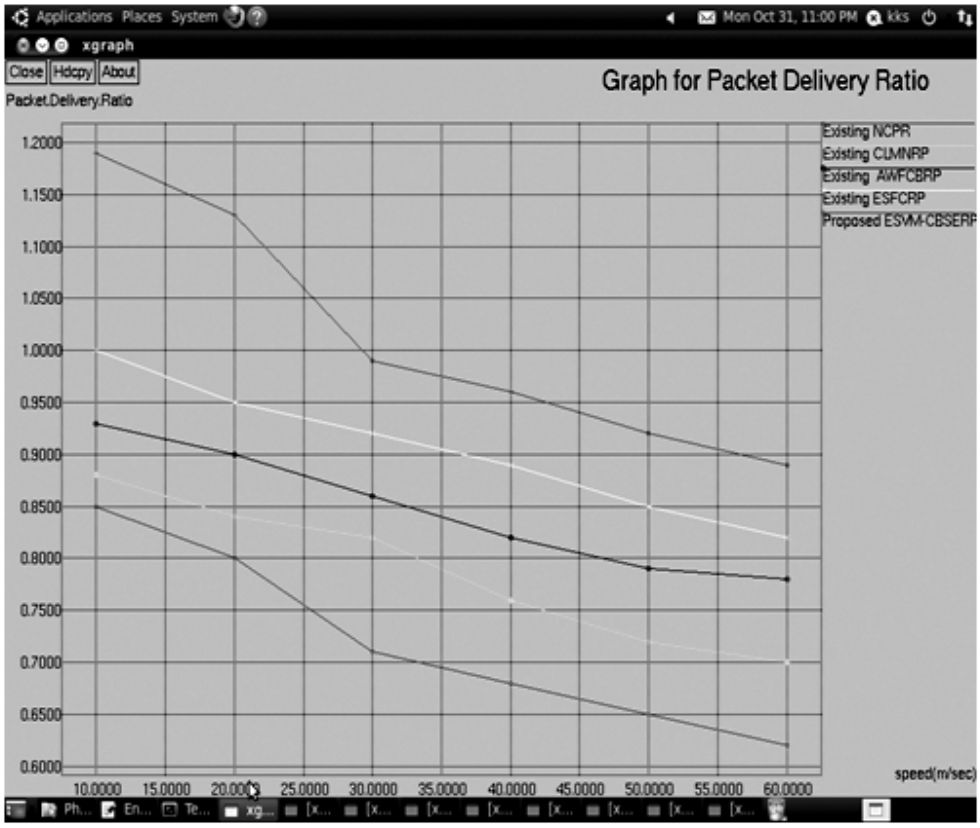


Figure 4: Packet Delivery Ratio vs. Speeds

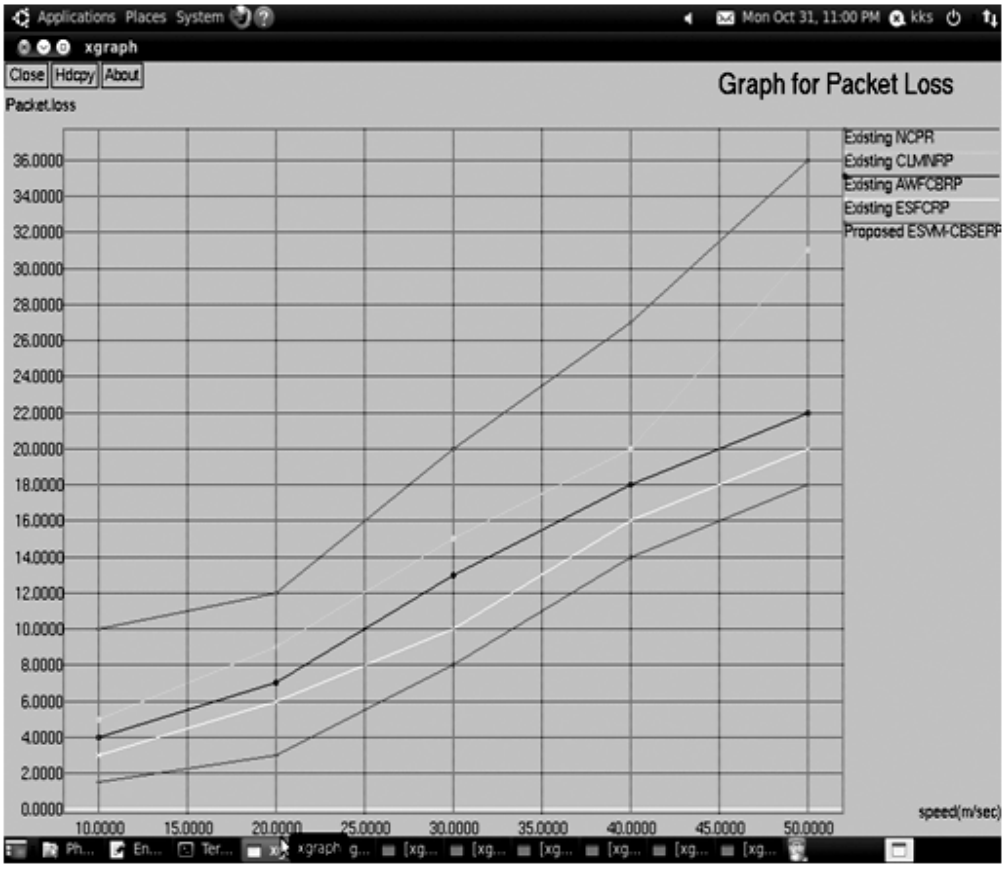


Figure 5: Number of Packets Loss vs. Speeds

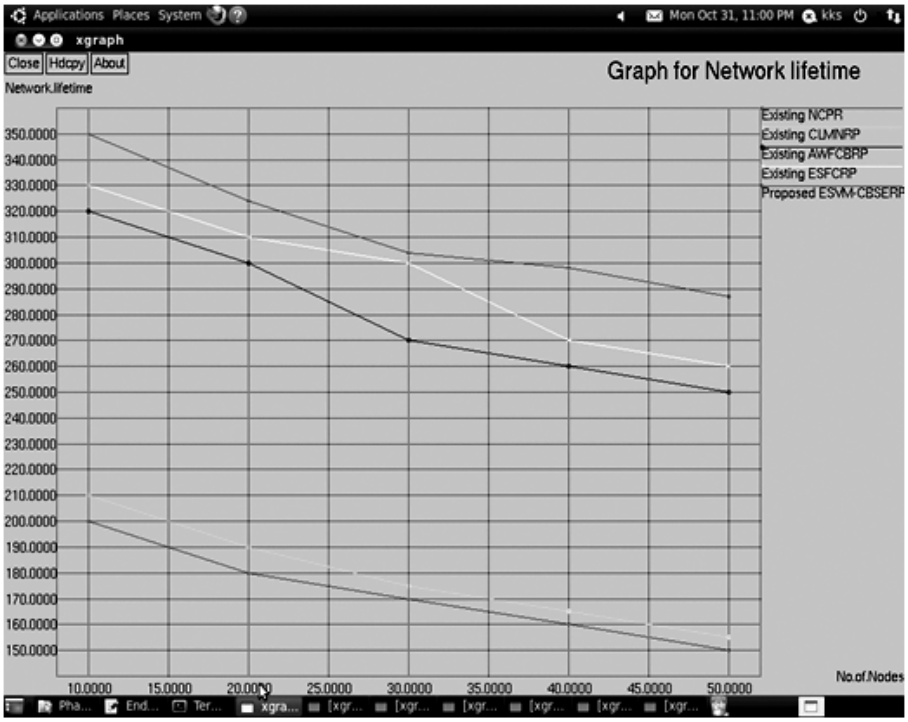


Figure 6: Network Life Time vs. Number of Nodes

4.4. Throughput

Figure 7 indicates the throughput estimation. The proposed ESVM-CBSERP achieves the higher throughput when compared with the other protocols are NCPR, ESFCRP, AWFCBRP, and CLMNRP. Due to increase in throughput, the convergence speed of packet transmission in proposed work removes if any congestion occurred for every transmission.

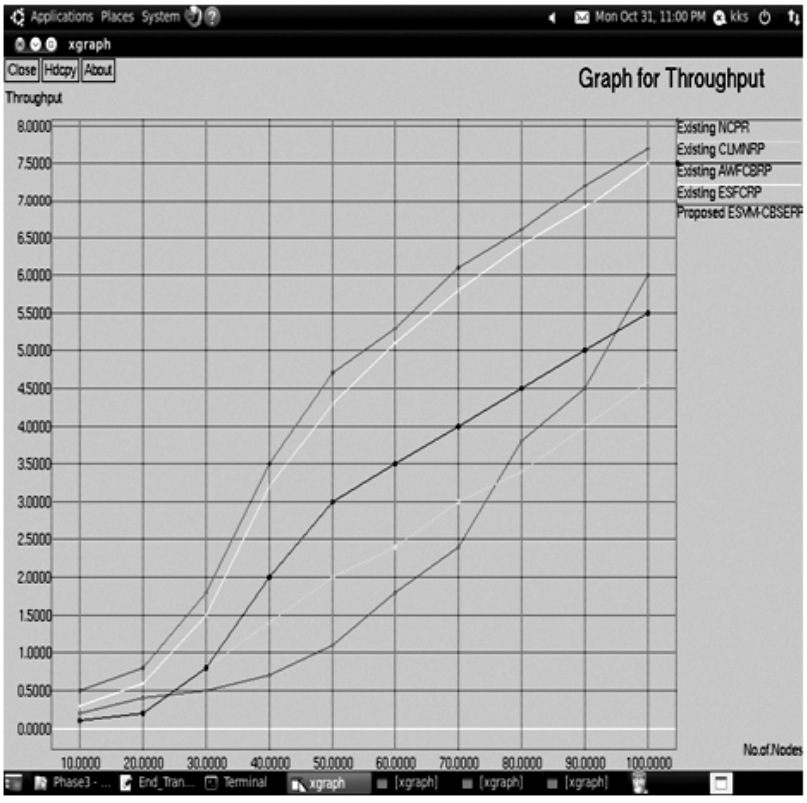


Figure7: Throughput Graph vs. Number of Node

4.5. Mean Delay

Figure 8 indicates mean delay vs. number of node. Proposed ESVM-CBSERP mean delay is decreased compared with the other communication approaches are NCPR, ESFCRP, AWFCBRP, and CLMNRP calculated. Present scheme monitors the priority of end to end delay in an every hop count packet transmission.

Figure 8: Mean delay vs. Number of node

4.6. Path Reliability

Figure 9 denotes the Packet reliability rate estimation. Beginning the results, the present ESVM-CBSERP protocol achieves high packet reliability rate than the existing schemes are NCPR, CLMNRP, AWFCBRP and ESFCRP since stability is maintained in every transmission.

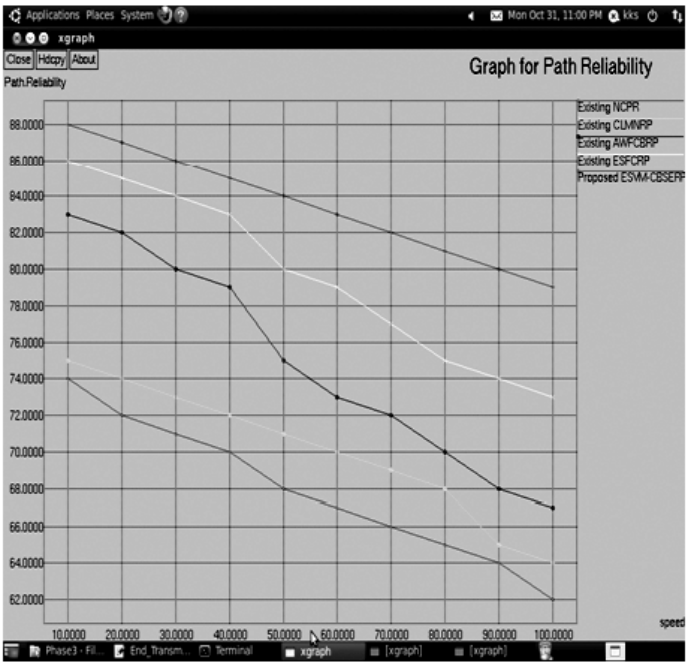


Figure 9: Path Reliability vs. Speed

4.7. End Transmission

In Figure 10 denotes the end transmission evaluation. The end to end transmission of proposed ESVM-CBSERP attains higher compared to existing schemes are NCPR, CLMNRP, AWFCBRP and ESFCRP because of high path reliability condition.

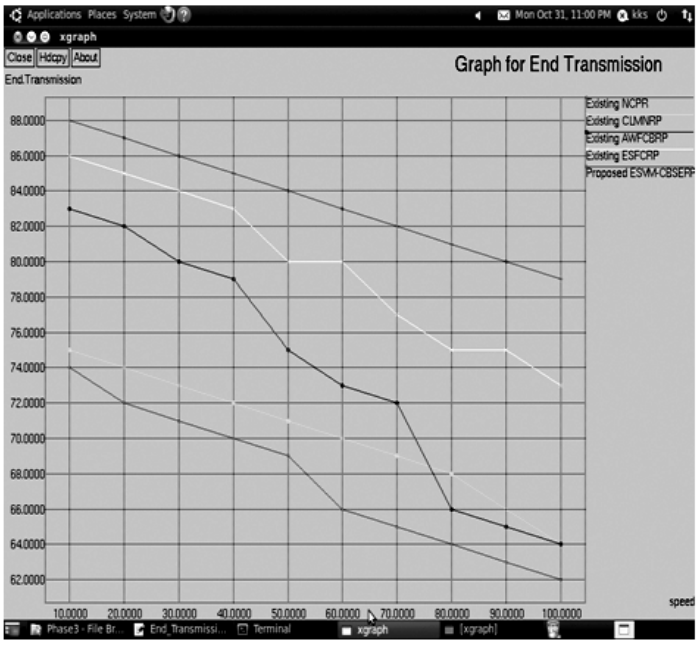


Figure 10: End Transmission vs. Speed (mbps)

4.8. End to End Delay

In Figure 9, indicates end to end delay estimation. The proposed ESVM-CBSERP has minimum end to end delay for each packet compared to existing schemes are NCPR, CLMNRP, AWFCBRP and ESFCRP. The pause time is reduced to minimize the delay between the packets.

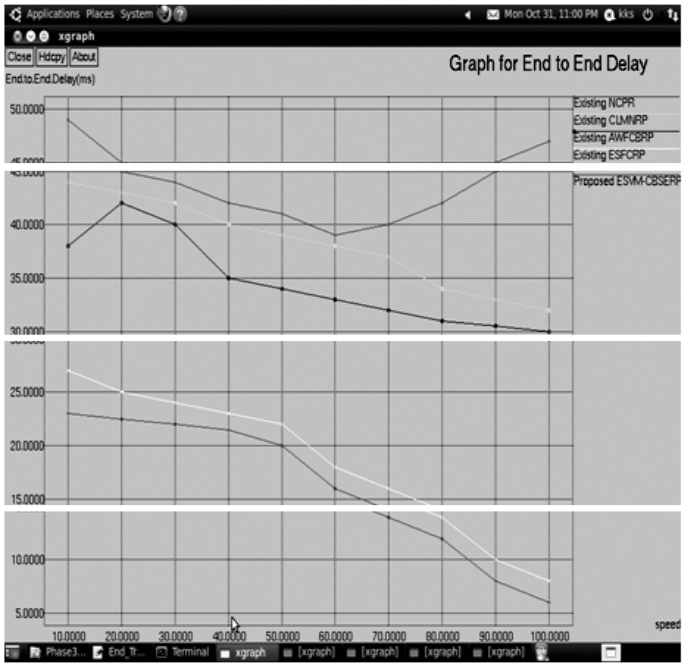


Figure 11: End to End Delay vs. Speed (mbps)

4.9. Communication overhead

In Figure 6, the time varies from 10 to 100. When increasing the time, the communication overhead of proposed ESVM-CBSERP has low than NCPR, CLMNRP, AWFCBRP and ESFCRP. This is achieved by employing the trustable packet loss ratio in the transmission process.

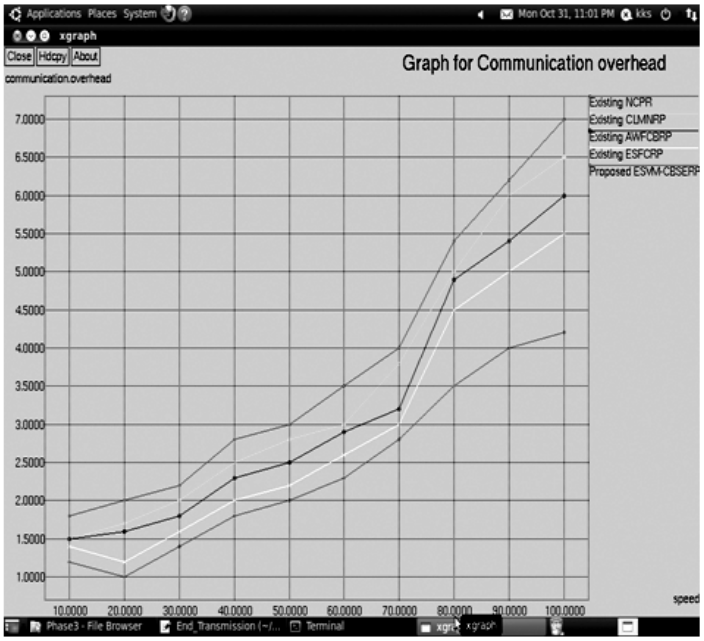


Figure 12: Communication overhead vs. Time

5. CONCLUSION

In this work, the ESVM-CBSERP is proposed and investigated as a complementary mechanism to reinforce secure knowledge delivery in an exceedingly mobile ad hoc network. the fundamental plan is to rework a secret message into multiple shares, then deliver the shares via multiple ways to the destination in order that even though a definite variety of message shares are compromised, the key message as an entire is not compromised. With the planned clustering algorithmic program, the novel mechanism for providing routing security in mobile ad hoc network implementing ones complement and cryptologic algorithmic program is mentioned. That may be embedded all told the routing protocols to produce security and to extend potency of the network. Simulation results showed that the clustering algorithmic program improves cluster's stability and also the planned ESVM-CBSERP provides superior performance with many benefits over previous routing protocol. the long run scope of planned mechanism is to be analyzed with relevance varied routing ideas and performance problems like delay, throughput, and measurability disturbance and packet delivery quantitative relation on the massive area networks.

REFERENCES

[1] Lin, H. & Labiod, H. (2006). INGEO: INdoor GEOgraphic routing protocol for MANETs. In Proceedings of the 3rd International Conference on Mobile Computing and Ubiquitous Networking, 2006.

[2] Yen, Y. S., Chao, H. C., Chang, R. S., & Vasilakos, A. (2011). Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs. Mathematical and Computer Modelling, 53(11–12), 2238–2250.

[3] Dvir, A., & Vasilakos, A. (2011). Backpressure-based routing protocol for DTNs. ACM SIGCOMM Computer Communication Review, 41(4), 405–406.

[4] Zou, C., & Chigan, C. (2009). On anonymous on-demand source routing protocol for MANETs. Wiley's Journal of Security and Communication Networks, 2(6), 476–491.

[5] S. Sivagurunathan, V. Mohan and P. Subathra,"Distributed Trust Based Authentication Scheme in A Clustered Environment Using Threshold Cryptography for Vehicular Ad Hoc Networks", International Journal of Business Data and Communication and Networking (IJBDCN), Vol.6 (2), 2010.

[6] R. Murugan and A. Shanmugam, "Cluster Based Node Misbehaviour Detection, Isolation and Authentication Using Threshold Cryptography in Mobile Ad Hoc Networks", International Journal of Computer Science and Security (IJCSS), Vol.6 (3), 2012.

[7] S. Yang, C.K. Yeo, B.S. Lee Toward reliable data delivery for highly dynamic mobile ad hoc networks IEEE Transactions on Mobile Computing, 11 (2012), pp. 111–124

[8] Ben Mahmoud, M. S., & Larrieu, N. (2013). An ADS-B based secure geographical routing protocol for aeronautical ad hoc networks. In Proceedings of the IEEE 36th Annual Computer Software and Applications Conference (COMPSAC).

[9] Sharon Ranjini, S., & Shine Let, G. (2013). Security-efficient routing for highly dynamic MANETS 2013. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249–8958, 2(4).

[10] Leinmuller, T., Maihofer, C., Schoch, E., & Kargl, F. (2006). Improved security in geographical adhoc routing through autonomous position verification. In 2006 Proceeding Vanet 06 of the 3rd International Workshop on Vechicular adhoc Networks.

[11] A. Rajaram, S. Gopinath, Optimized Multicast Routing Scheme for Mobile Ad hoc Networks, Journal of Theoretical and Applied Information Technology, 59 (2014), pp. 213–221

[12] R. Aquino-Santos, L.A. Villaseñor-González, V. Rangel-Licea, A. González-Potes, M.A. García-Ruiz, A. Edwards-Block A Novel Topological Multicast Routing Algorithm (ToMuRo) Journal of Applied Research and Technology, 8 (2010), pp. 44–55

[13] S. Jamali, L. Rezaei, S.J. Gudakahriz, An Energy-efficient Routing Protocol for MANETs: a Particle Swarm Optimization Approach, Journal of Applied Research and Technology, 11 (2013), pp. 803–812

[14] Shen, H., & Zhao, L. (2013). ALERT: An anonymous locationbased efficient routing protocol in MANETs. IEEE Transactions on Mobile Computing, 12(6), 1079–1093.

[15] El Defrawy, K., & Tsudik, G. (2011). ALARM: Anonymous location-aided routing in suspicious MANETs. Mobile Computing IEEE Transactions, 10, 1345–1358.

[16] Lyu, C., Gu, D., Zhang, Y., Lin, T., & Zhang, X. (2013). Towards efficient and secure geographic routing protocol for hostile wireless sensor networks. International Journal of Distributed Sensor Networks, Networks, 2013.

[17] Zhang, X. M., Gu, D., Zhang, Y., Lin, T., & Zhang, X. (2015). Interference-based topology control algorithm for delay-constrained mobile Ad hoc networks. IEEE Transactions on Mobile Computing, 14(4), 742–754.

[18] Song, Y., Liu, L., Ma, H., & Vasilakos, A. V. (2014). A biologybased algorithm to minimal exposure problem of wireless sensor networks. IEEE Transactions on Network and Service Management, 11(3), 417–430.

[19] Liang, L., Song, Y., Zhang, H., Ma, H., & Vasilakos, A. V. (2015). Physarum optimization: A biology-inspired algorithm for the steiner tree problem in networks. IEEE Transactions on Computers, 64(3), 819–832.

[20] J. M. Ng and Y. Zhang, "A mobility model with group partitioning for wireless ad hoc networks," in Proceedings of the 3rd International Conference on Information Technology and Applications (ICITA '05), pp. 289–294, Sydney, Australia, July 2005.