A Secured MANET Using Multicast Routing Protocols and Semi Markov Process

Maragatharajan M. and Balakannan S. P.

Department of Information Technology, Kalasalingam University, Tamilnadu, India
E-mail: maragatharajanm@gmail.com; balakannansp@gmail.com

Received 18 January 2018; Accepted 22 March 2018;
Publication 16 April 2018

Abstract

Reliable data delivery is essential in the mobile ad hoc network (MANET) and the devices change their positions very frequently since they do not have any fixed infrastructure. In this paper, we have proposed multicast routing protocols for military communications. The military communications with MANET require data security. We using one of the most widely used algorithms Neighbor supporting Ad hoc Multicast routing protocol which is Mesh-based routing algorithm. Semi Markov process is used to develop the node behavior model for network survivability. In this work, reliable data delivery is obtained for the MANET by estimating the present performance of the network through isolating the forwarder node in Semi Markov process.

Keywords: MANET, NSMP, Markov Process.

1 Introduction

Wireless Mobile ad hoc networks are suitable in situations where there is no system foundation accessibility and when there is a requirement for individuals to impart utilizing cell phones. Since MANETS depend on transmission, a secured method for message transmission is critical to ensure the protection of the information. An insecure ad-hoc network at the edge of a current correspondence foundation may conceivably make the whole system end up

Journal of Cyber Security, Vol. 7_1, 53–68.
doi: 10.13052/jcsm2245-1439.715

noticeably defenseless against security breaks. The inherent idea of remote impromptu systems makes them extremely powerless against assaults running from uninvolved listening stealthily to dynamic obstruction. In mobile ad hoc networks, there is no focal organization to deal with recognition and anticipation of peculiarities. Be that as it may, the vast majority of the current key administration plans are not attainable in specially appointed systems since open key foundations with a unified accreditation expert are difficult to send [1, 2]. Subsequently, cell phones characters or their goals can't be foreordained or checked. Hence hubs need to participate for the trustworthiness of the operation of the system. However, hubs may decline to coordinate by not sending packets for others for narrow-minded reasons and not have any desire to debilitate their assets. Due to factors like mobility of nodes, mode of operations, short processing power and limited resource availability make the task complicated [3].

The armed phases in a mobile ad hoc network are specifically fascinating and difficult [4]. In a war field scenario with an unfriendly situation, we have a lot of things to consider and stringent limitations than in a MANET for educational purposes or commercial purposes. For example, a war field situation may have a lot of needs about the information security. The routing process also has to be more trustworthy and exact, with problems regarding bandwidth, radio range, power consumption and security.

The scenario consists of a huge number of tanks that are travelling through an area in an aggressive situation. At that time, transferring messages among the tanks can be achieved with the help of a MANET. To achieve data security, the data must be secure besides every probable danger. The chance of immediate modifications such as attractive opponents in fight or rest in the movement because of a hazard shouldn't disturb the message. The communication should be maintained at all times. The important parameters which we concern while we choose a routing protocol are the Hostile enemy, Trust models, QoS control, Radio power usage restrictions and Robustness.

The nodes of a MANET is not stable and to minimize the overhead of routing procedures, the conventional routing protocols like Ad hoc On-demand Distance Vector routing protocol (AODV), Dynamic Source Routing protocol (DSR) and Destination sequenced Distance Vector routing protocol (DSDV) are not adequate for MANET. One of the main reasons is the predetermination of a whole route before data delivery. The revelation and recuperation systems may consume more energy and time. Likewise, if the path between the nodes is broken, then the information packets will get lost or be postponed for quite a while until the restoration of the path. It will cause interference in data transfer.

A new ad hoc multicast routing protocol called Neighbor-Supporting Multicast Protocol (NSMP) is mesh based protocol [5]. NSMP embraces a working structure to upgrade versatility against portability. What's more, NSMP uses hub territory to lessen the overhead of course disappointment recuperation and work upkeep. NSMP likewise endeavors to enhance course effectiveness and diminish information transmissions. Our recreation comes about demonstrate that NSMP conveys parcels effectively while generously decreasing control overhead in different conditions.

Network Survivability is a crucial part of dependable communication services [7]. It is nothing but the capacity of a system to satisfy its main goal in an opportune way within the sight of dangers; for example, attacks or large-scale disasters. The fundamental goal of the network survivability is associated with topology wherever it is possible, especially inside the sight of malicious attacks and random failures. A typical rule is that the node has dynamic neighbours, the node is associated with the system 'physically' through remote connections. In any case, it can scarcely hold in a genuine system by considering potential node misbehaviour and random failures. Therefore, the presence of node misbehavior leads to a challenge of the network survivability. Semi Markov procedure can portray the advancement of node behaviours. The cooperation of the node is to be examined by stochastic property of the model.

In a mobile ad hoc network, node collaboration effort in a directing system is a basic need to keep up channel life time [5]. While all the nodes are autonomous; it might choose the proper behaviour in the system itself. When taking into considerations of all possible effects in different misbehaviours, all the nodes can be classified into following four different states.

- *Cooperative State (C)*: A device obeys all steering and sending decides that is having the capacity to start and react to route identification effectively.
- *Selfish State (S)*: A device can begin and respond to the route disclosures for its own inspirations yet may not send the information packets to others.
- *Malicious State (M)*: The Denial of Service (DoS) attacks will be dispatched by a device on the network layer that is very useful for guiding them; however, vacillate in sending information.
- *Failure State (F)*: A device can't start or react to route disclosures.

The remaining part of the paper is organized in the following way. The Neighbor Supporting Multicast Routing Protocol mechanism described in

Section 2 and Section 3 briefly describes Semi Markov process and the classification of nodes based on the behaviour model. In Section 4, the investigational arrangement and effects are given, and Conclusion and future works are presented in Section 5.

2 Neighbor-Supporting Multicast Routing Protocol Mechanism

Neighbor-Supporting Multicast Protocol (NSMP) is a vigorous, less overhead and productive convention. We utilize the working framework since strength against connecting disappointments is a vital property of specially appointed multicast directing. Communicates are costly operations in impromptu systems. NSMP limits the recurrence of control message communicates. Communicates are once in a while utilized for starting course foundation or a system parcel repair. For ordinary and occasional work systems for upkeeps, control messages achieve just sending hubs and their neighbor hubs. In choosing another course, NSMP inclines toward a way that contains existing sending hubs. Along these lines, NSMP upgrades the course productivity by lessening the quantity of sending hubs.

NSMP performs two sorts of course recuperation: flooding course revelation and nearby course disclosure. For routine way systems of support, NSMP utilizes neighborhood course revelation which is confined just to a little arrangement of versatile hubs straightforwardly identified with a multicast gathering. For an underlying course foundation or a system parcel repair, NSMP at times performs flooding course disclosure in which control packets are communicated by all nodes. For extensive associations, routine way systems for upkeeps happen ordinarily more frequently than the underlying way foundation, and the sparing by confined way support could be sizable.

Multicast Mesh Creation

A multicast work of a gathering comprises of sources, recipients, sending hubs, and connections associating them. These hubs in a multicast work are called work hubs.

Figure 1 Accept that nodes 6 and 13 are beneficiaries of a multicast gathering. At the point when hub 4 joins the gathering as a source, it communicates a FLOOD REQ parcel. Node 5 gets the packet and communicates it. At the point when hub 6 gets the FLOOD REQ parcel, it forwards a REP packet to its upstream, node 5. At the point when node 5 gets the REP parcel, it realizes

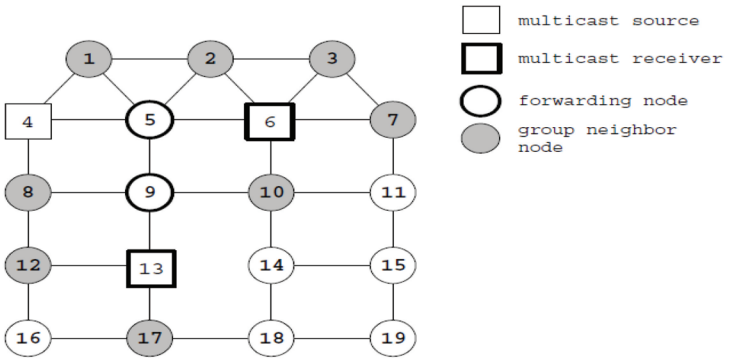

Figure 1 Multicast Mesh Creation.

that it is on the multicast work and transfers the packet to its upstream, hub 4. Essentially, hub 13 likewise sends a REP parcel and hub 9 turns into sending nodes.

At the point when a source transmits a DATA parcel, just sending nodes hand-off the packet, with the goal that the parcel is conveyed to collectors along a setup work. Presently let us consider neighbor nodes of the multicast work. Neighbor nodes are nodes that are specifically associated with no less than one work hub. In Figure 1 hubs, 1, 2, 3, 7, 8, 10, 12, and 17 are the neighbor nodes. Sending hubs and gathering neighbor nodes lose their capacity unless they are invigorated inside predefined timeout period.

Multicast Mesh Maintenance

a) Local Route Discovery:

Each source intermittently transmits a LOCAL REQ parcel, and just work hubs and gathering neighbor hubs hand-off the packet. Along these lines, all hubs two bounces far from the work hubs get the LOCAL REQ packet. This component can decrease control overhead, and because of hub region, it repairs most connection disappointments caused by hub developments. REP Packets to LOCAL REQ packets are transferred to a Source similarly as REP parcels to FLOOD REQ parcels. Sending hubs and gathering neighbor hubs along a multicast work are refreshed as REP parcels are handed-off to a source.

For instance, expect that a disappointment jumps out at a connection (9, 13) in Figure 2. Hub 4 will, in the end, send a LOCAL REQ packet since each source occasionally performs nearby course revelation. At the point when hub 8 gets the packet, it communicates the parcel since amass neighbor hubs

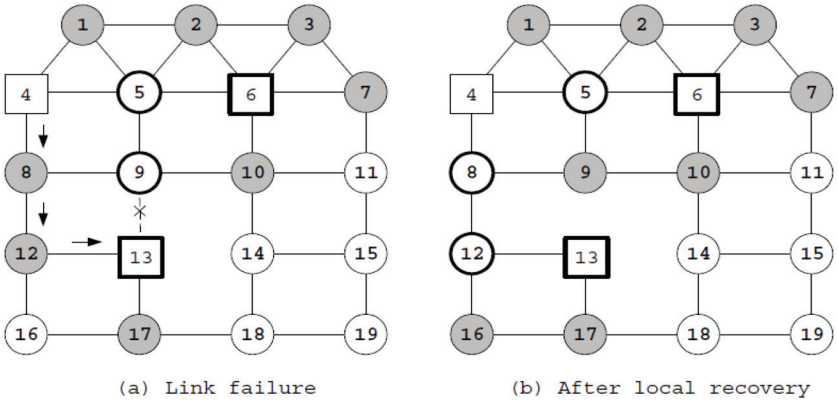

Figure 2 Multicast Mesh Maintenance.

transfer LOCAL REQ parcels. At the point when hub 12 along these lines communicates the parcel, hub 13 gets it and sends a REP packet to fabricate another course to the source. The repaired work appears in Figure 2 (b). Note that over 30% of the hubs (i.e. six hubs) in Figure 2 (a) don't re-communicate the LOCAL REQ packet. Nearby course disclosure guarantees bringing down control overhead, however, it doesn't repair all connection disappointments. Assume that a connection (8, 12) in Figure 2 (b) fizzled.

Nearby course disclosure can't repair this connection disappointment. With sensible system availability, notwithstanding, locally unrecoverable connection disappointments happen less often than interface disappointments that can be repaired by neighborhood course revelation.

b) Flooding Route Discovery:

NSMP utilizes flooding course revelation in a few cases. At the point when a hub turns into another source, it sends a FLOOD REQ packet keeping in mind the end goal to make an underlying cross-section. In NSMP, a hub inside two jumps far from work hubs can join the gathering as a beneficiary by answering to a LOCAL REQ packet. Be that as it may, a hub more than two bounces far from the work hubs must surge a MEM REQ parcel. Furthermore, organize segments just can be recouped by FLOOD REQ packets.

3 Semi Markov Process

Surviving in the network is the ability of an organization to satisfy its main goal, in a right way, within the sight of attacks, failures or accidents.

The abundance packet loss in view of failure and data rate can be considered as the survivability execution assessment. It is essential for established network executions assessment for data arranges and not as fundamentally indicate for ad hoc networks [10]. Based on the survivability performance, the nodes can be classified into four states as a Cooperative state (C), Selfish State (S), Malicious State (M) and failure State (F).

Especially, we concentrate just two sorts of behaviours in this paper: Jellyfish and Blackhole attacks [7]. Jellyfish attack does not defy the principles of the directing protocols. But it is unquestionably genuine that the jellyfish attack is hard to recognize from congestion and packet losses that happen normally in a network, and accordingly, it is hard and resource-consuming to detect. Also, it reorders delays and/or drops the data packets. An attacker can drop received routing messages, rather than handing-off them as the protocol requires, all together decreasing the amount of routing data accessible to all nodes. This is called blackhole attack and a basic approach to play out a Denial of Service (DoS).

Based on the classification of nodes, we characterize the condition of the node, {C, S, M, F}. A Stochastic model can be created to analyze the disclose effects of nodes. Always the future behavior of the node is based on current behavior and not on previous behaviors. So we can build up a Semi Markov Model to detect the behavior of nodes. A node may change from one state to another due to the following reasons [8].

Node at Start	Node at End	Reason
C	F	Energy exhaustion, Misconfiguration
	S	Inclined to be arranged intentionally as a narrow-minded one for the sack of power saving
S	C	Proper configuration
	M/F	Due to being compromised/Power depletion
M	F	No longer considered
F	C	Recovered and responds to routing operations

Let S_n denotes the state at transition time t_i, and then we have

$$K_r(S_{n+1} = s_{n+1} | S_0 = s_0, \ldots, S_n = s_n) = K_r(S_{n+1} = s_{n+1} | S_n = s_n) \quad (1)$$

Where $S_i \; \varepsilon \; \delta$ for $0 \leq i \leq n + 1$, constitutes a Markov chain with state space δ. But the transition time from one state to another state is totally based on random behavior of a node and it is very difficult to characterize transition

time by exponential distributions. Therefore we use a SMP (X(t)) to model node behavior transitions and it is given by

$$\mathrm{X(t)} = \mathrm{S_n} \text{ where } \mathrm{t_n} \leq \mathrm{t} \leq \mathrm{t_{n+1}} \tag{2}$$

X(t) denotes the state of process during the period from the most recent transition and $\{\mathrm{S_n}\}$ is called EMC (Embedded Markov chain) of the process X(t).

The SMP model assumes memory-less property and it can be used to define the random threats caused by node behaviors. So we can define time heterogeneous Semi Markov kernel model by

$$\mathrm{Q_{xy}(t)} = \mathrm{K_r(S_{n+1} = vj,\ T_nv < t | S_n = i)} = \mathrm{k_{ij}F_{ij}(t)} \tag{3}$$

Based on these assumptions, a probability matrix can be created. It contains the probability values of changes in states of each node.

$$\mathrm{PM} = \begin{pmatrix} 0 & \mathrm{p_{cs}} & \mathrm{p_{cm}} & \mathrm{p_{cf}} \\ \mathrm{p_{sc}} & 0 & \mathrm{p_{sm}} & \mathrm{p_{sf}} \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

In the above matrix $\mathrm{p_{fc}} = \mathrm{p_{fm}} = 0$ means the failure node never become as a selfish or malicious node. Likewise $\mathrm{p_{mf}}$ = 1 means if the malicious node is no longer considered, it will become as a failure node. Also $\mathrm{p_{fc}} = 1$ mean the failure node can be recovered and responded for routing. As the limiting probabilities like $\mathrm{P_i}$, $\mathrm{P_j}$ stanf for long term average distributions of node behaviors and they are more accessible. So they can be used directly as $\mathrm{P_c}$, $\mathrm{P_b}$ and etc with same initial energy.

The essential uneasiness for a logical model is whether it can be used to assess or anticipate future practices. In similar manner, the representation itself must be satisfactory for data scattering, given complete or inadequate information.

A numerical arrangement may be used to tackle by adjusting the passing assignments in a distinct time space as [7].

$$\mathrm{P_{xy}(st)} = (1 - \mathrm{H_x(st)})\delta_{\mathrm{xy}} + \mathrm{iQ_{xy}(st)P_{ly}(st - xt)} \tag{4}$$

Where h is the discretization step. Also $\mathrm{Q_{xy}(st)}$ can be given as

$$\mathrm{Q_{xy}(st)} = \mathrm{h^{-1}(A(xt) - B((x-1)h))} \text{ for } \mathrm{x} > 1 \tag{5}$$

Where A and B are the empirical distribution functions. By utilizing this strategy, when all states move and time cases are accessible then Qxy(st) and Pxy(st) can be calculated [9, 10].

The Semi Markov Process $\{X(t)\}$ associated state space δ and the transient distribution $P_{ij}(t)$ converges to a limiting probability P_j as $t \to \infty$, further P_j can be calculated by

$$P_j = \lim_{t\to\infty} P_{ij}(t) = \frac{\pi_j E[T_j]}{\sum_{1\varepsilon\ \delta}\ \pi_l E[T_l]} \tag{6}$$

Where π is the stationary distribution. Due to node misbehavior, any device employed supportively diverges every time, depends upon variety of elements like resource level, node movement and attack. With the help of overall Semi Markov Procedure to exhibit the advancement of device practices, we can assess the transient and compelling chance of a device being in a supportive situation.

3.1 Node Isolation

Node Isolation is a solution for node misbehavior and failures because of communication between nodes are totally subject to routing information [10]. In this regard, the failure device may be distinguished by routing procedures and they will be segregated or detached from the network. The node isolation can be considered for the following scenarios:

i. Failure node with no routing capacity
ii. Selfish node with hesitance in forwarding mechanism packages
iii. Mischievous node with focus of diverting routing procedures.

The probability misbehaving nodes with node isolation property of a network can be calculated as follows [11, 12].

$$P_x(D_c = 0|D = d) = 1 - (1 - P_b)^d + (1 - P_c - P_b)^d \tag{7}$$

Where P_c is the probability of a node being in a cooperative state and P_b is the probability of a node launching blackhole attack. Also d is degree of a node. From the above equation, we can see the immediate effect of node misbehaviors activities on the node isolation probability as the server the node misbehaviors present in a network, the less likely that a node's neighbors are cooperative, and thus, the more likely that the node is isolated from the network. For a given $P_{b,}$ the cooperative probability P_c plays an important role in determining the connectivity of individual nodes. For example, when $P_c = 0$,

$P_x(D_c = 0|D = d) = 1$, which means a node isolation because of no cooperative neighbors, and when $P_c = 1$, $P_x(D_c = 0|D = d) = 0$, which means that node isolation is not caused by any node misbehaviors and failures.

The value of P_{ij} can be calculated using Heuristic estimation of transition probabilities. For that we need to estimate $E[T_{cf}]$ by considering two factors such as energy consumption and node mobility. Assume T_{CL} be the lifetime of a cooperative node and T_{in} is the residence times of a cooperative node then $E[T_{cf}]$ can be defined as

$$E[T_{cf}] = E[\min(T_{CL,}T_{in})] \leq \min(T'_{CL}, T'_{in}) \tag{8}$$

Where T'_{CL} is the mean of node lifetime and T'_{in} is the average lifetime. Further T'_{CL} can be defined as

$$T'_{CL} = \frac{Einit}{\alpha P_{Tx} + (1-\alpha)P_{Rx}} \tag{9}$$

Where α is the ratio between number of transmitting packets and that of processed packets.

4 Scenario Study and Simulation Results

The network performance due to misbehaving nodes, network survivability and simulation results are analyzed in this part. P_T and P_R represent average transmitting and receiving power.

$$E[T_{sf}] \leq \min(\varepsilon(1-\beta)^{-1}\ T'_{CL,}\ T'_{in}) \tag{10}$$

To estimate $E[T_{mf}]$, the node can be compromised at any time and become malicious after an average period T'_a. So

$$E[T_{mf}] = \min(T'_{CL}/2 - T'_a, T'_{in)} \tag{11}$$

Other expected transition times are approximated by,

$$E[Tcs] = (1-\varepsilon)T'_{CL} \tag{12}$$

By using Equation (6) we can calculate the value of $E[T_i]$. We obtain the TPM of our Semi Markov model is given as,

$$PM = \begin{pmatrix} 0 & 0.525 & 0.071 & 0.404 \\ 0.756 & 0 & 0.022 & 0.222 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Then $E[T_{ij}]$ can be calculated using (8) – (12). The values are as follows since we know the value of P_{ij}.

$$E[T_c] = 142.2, E[T_s] = 45.9, E[T_m] = 51.7, E[T_f] = 60.$$

We obtain the limiting probabilities Pi using (6),

$$P_c = 0.06877, P_s = 0.1167, P_m = 0.0207, P_f = 0.1750$$

4.1 Scenario Study

The following assumptions are used to succeed the simulations [10].

- The initial energy of all the nodes in the network in equal.
- To convert selfish node into cooperative node nuglet counter scheme [14] will be implemented.
- The probability of node to be exchanged by an outside attacker is same for both cooperative and selfish node.
- The residence time of any node in the network is irregular and it is relying upon the development pattern of individual node.

4.2 Simulation Set up

To analyze the performance of NSMP with Markov process, we simulate the algorithm in NS-2 and compared it with NSMP protocol. The basic parameters used in this simulation are given in Table 1.

4.3 Simulation Results

i) Throughput

It is characterized by the collective amount of packages sent to the target over the aggregate simulation time.

Table 1 Simulation Parameters

Parameter	Value
MAC protocol	IEEE802.11
Mobility Model	Random way point (RWP)
Number of Nodes	100
Simulation Time	900 sec
Propagation Model	Two-ray Ground
Packet Size	256 Bytes
Transmission Range	250 m
Traffic Type	Constant Bit Rate (CBR)

ii) End-to-End delay

The average time takes data to influence the target node from the source node. This incorporates all conceivable delays created by defending for the duration of route discovery latency. This metric is figured by subtracting time at which first data packet was transmitted by the source from a time at which first data packet received at the destination.

End-to-End delay = T/N, where T resembles the aggregate of the period consumed to deliver for each destination, and N is the amount packages acknowledged by the all cause nodes.

iii) Package transfer ratio

Package transfer ratio is characterized as the proportion of the amount of packages acknowledged by the destinations to those generated by the sources.

Packet Delivery Ratio = N1/N2, where N1 is the total amount of information packages acknowledged by every target and N2 is the total amount of information packages originated from every cause node.

Figure 3 illustrates the performance of NSMP and NSMP with Markov process. When we include Markov process in NSMP, it performs well and it gives better Package delivery ratio.

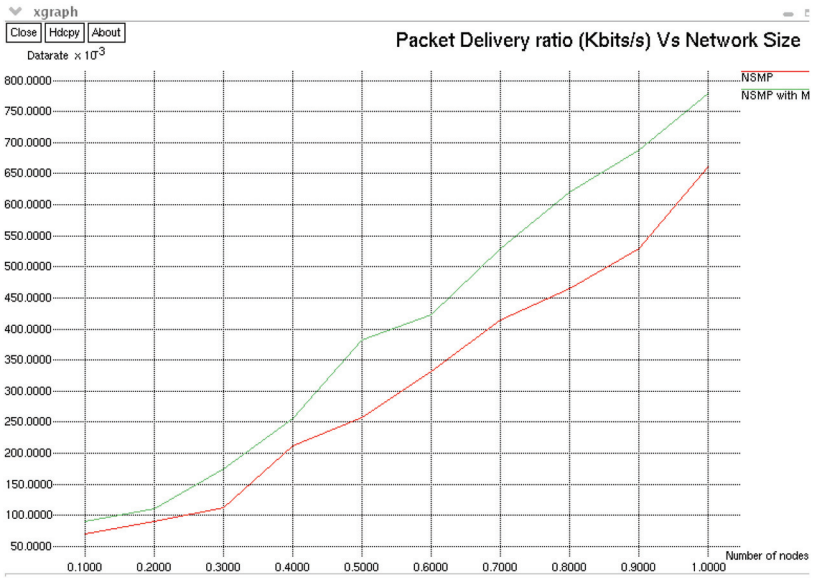

Figure 3 Packet Delivery Ratio.

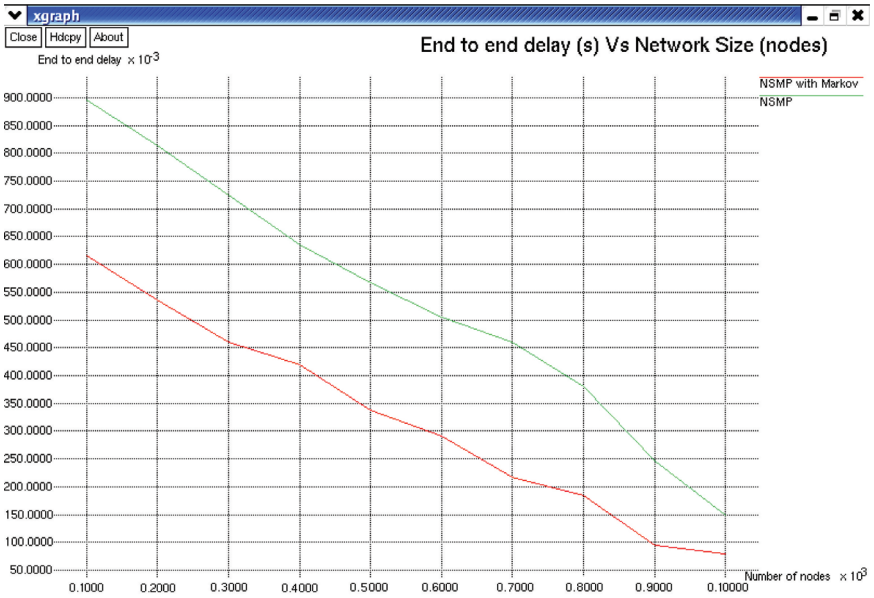

Figure 4 End to end Delay.

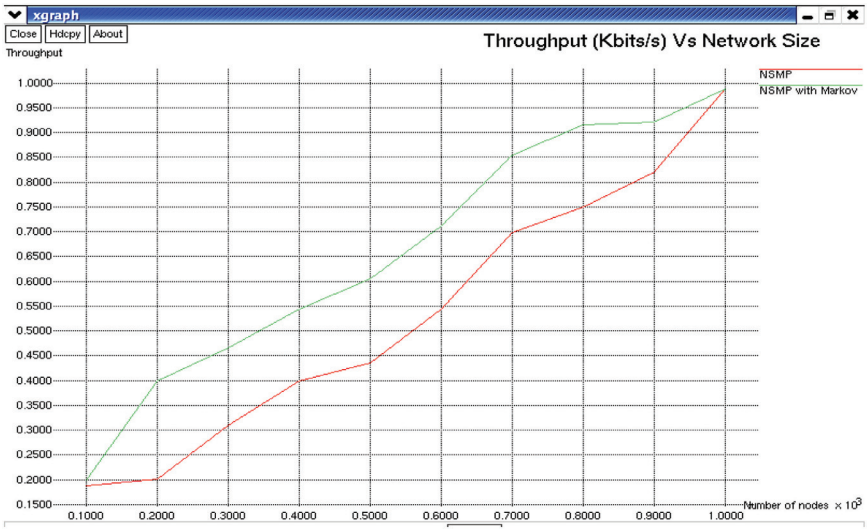

Figure 5 Throughput.

Figure 4 shows the delay comparison between NSMP and NSMP with Markov process. From this, we can see the overall delay of MANET can be reduced when we incorporate the Markov chain process with NSMP protocol.

Figure 5 illustrates throughput comparison between NSMP with Markov process. The Throughput of NSMP and with Markov process is linearly increased with the number of nodes increases.

5 Conclusion and Future Works

This paper proposed a solution for consistent data delivery for MANET. The NSMP routing method gives better Packet delivery ratio, delay and throughput. To improve the security services of MANET, the Markov chain process is included along with the protocols which are used to identify the malicious node and selfish node. The simulation results show that NSMP with Markov process are comparatively better than normal NSMP protocol.

The protocol was analyzed with Markov chain process which is based on past behavior of the node. Instead of Markov chain, a trust-based model can be designed to analyze the node behavior. It is used to give more accurate information about the individual nodes.

References

[1] Durkadevi, K., Maragatharajan, M., and Balakannan, S. P. (2014). "Reliable Data Delivery for highly Dynamic MANETs Using Adaptive Demand Driven Multicast Routing Protocol (ADMR)," *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)*, 2(1).

[2] Thanikaivel, B., and Pranisa, B. (2012). Fast and secure data transmission in MANET. In *International Conference on Computer Communication and Informatics (ICCCI),* 1–5.

[3] Curtmola, R., and Nita-Rotaru, C. (2009). BSMR: Byzantine-resilient secure multicast routing in multihop wireless networks. *IEEE Transactions on Mobile Computing*, 8(4), 445–459.

[4] Halvardsson, M., and Lindberg, P. (2004). Reliable group communication in a military Mobile Ad hoc Network. *reports from MSI*, School of Mathematics and Systems Engineering, Vaxjo University.

[5] Xing, F., and Wang, W. (2010). On the survivability of wireless ad hoc networks with node misbehaviors and failures. *IEEE Transactions on Dependable and Secure Computing*, 7(3), 284–299.

[6] Lee, S., and Kim, C. (2000). Neighbor supporting ad hoc multicast routing protocol. In *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing,* 37–44.

[7] Jia, W. K., Chen, C. Y., and Chen, Y. C. (2014). ALEX: an arithmetic-based unified unicast and multicast routing for MANETs. In *Wireless Communications and Networking Conference (WCNC)*, 2114–2119.

[8] Butty, N. L., and Hubaux, J. P. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications*, 8(5), 579–592.

[9] Rayner de Melo Pires, Sergio Zumpano Arnosti, and Alex Sandro Roschildt Pinto (2016) "Experimenting Broadcast Storm Mitigation Techniques in MANETs", In *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS)*, 5868–5877.

[10] Paul, K., Roychoudhuri, R., and Bandyopadhyay, S. (2000). Survivability analysis of ad hoc wireless network architecture. In *Mobile and Wireless Communications Networks,* 31–46. Springer: Berlin, Heidelberg.

[11] Mannie, E., and Papadimitriou, D. (2006). Recovery (protection and restoration) terminology for generalized multi-protocol label switching (GMPLS). IETF RFC 4427. Available at: http://www.ietf.org/rfc/rfc4427.txt

[12] Li, X. Y., Wan, P. J., Wang, Y., and Yi, C. W. (2003). Fault tolerant deployment and topology control in wireless networks. In *Proceedings of the 4th ACM International Symposium on Mobile ad hoc Networking & Computing*, 117–128.

[13] Bettstetter, C. (2002). On the minimum node degree and connectivity of a wireless multihop network. In *Proceedings of the 3rd ACM International Symposium on Mobile ad hoc Networking & Computing*, 80–91.

[14] Caballero-Gil, P., Molina-Gil, J., Hern ndez-Goya, C., and Caballero-Gil, C. (2009). Stimulating cooperation in self-organized vehicular networks. In *15th Asia-Pacific Conference on Communications*, 346–349.

Biographies

Maragatharajan M. received his Bachelor degree in Electronics & Communication Engineering from Anna University by 2007. He has received his Master degree in Information Technology from Kalasalingam University, 2010. He has worked as a Project Associate in TIFAC CORE in Network Engineering, Kalasalingam University from 2007 to 2008. Currently, He is working as an Assistant Professor in the Department of Information Technology, Kalasalingam University. His areas of interest are Ad-hoc Networks, Wireless Networks, and Network Security.

Balakannan S. P. received his Ph.D. degree from the Department of Electronics and Information Engineering at Chonbuk National University, South Korea (2010). He has received his master degree (5 years integrated) from the Department of Computer Science and Engineering, Bharathiar University, India, in the year 2003. He has worked as a Project Assistant in Indian Institute of Technology (IIT), Kharagpur, India from 2003 to 2006. Currently, he is working as Assistant Professor in the Department of Information Technology, Kalasalingam University, Tamilnadu, India. His areas of interest include Wireless Network, Network Coding, Cloud & Green Computing, Cryptography, and Mobile Communication.