Chapter 31
A Novel Approach for Non-cooperative Node Detection and Avoidance Using Reputation-Based Scheme in Mobile Ad hoc Network

Chandrima Chakrabarti, Ananya Banerjee, Sanchari Chakrabarti and Angana Chakraborty

Abstract A mobile ad hoc network (MANET) is a collection of wireless mobile nodes that form a dynamic network without the need for any infrastructure. Due to the dynamic nature of MANET, it is prone to different kinds of malicious attacks. In order to pursue secure communication in such networks, there are many research solutions proposed for detecting and avoiding such malicious activities. As we know, MANET works properly if participating nodes cooperate in routing and forwarding. However, a node may decide not to cooperate just to save its resources but still use network to relay its traffic. In this scenario, we propose a reputation-based strategy to detect non-cooperative or selfish nodes and to select proper forwarder node for improving overall packet delivery of the network. Moreover, our proposed solution ensures data integrity. We have also done survey and performance analysis on some existing malicious attacks detection and prevention techniques available. The entire simulation has been done using the Network Simulator (NS-2) (http://www.isi.edu/nsnam/ns/) and simulation results show better delivery compared to some of other existing techniques discussed in the papers by Khamayseh et al. (J Netw 7(1):116–125, 2012), Marti et al. (Proceedings of International

C. Chakrabarti (✉) · A. Banerjee
CSE Department, Narula Institute of Technology, Agarpara, Kolkata 700109, India
e-mail: chandrima.narula@gmail.com

A. Banerjee
e-mail: ananyabanerjee.narula@gmail.com

S. Chakrabarti
Brahmananda Keshab Chandra College, Baranagar, Agarpara, Kolkata 700109, India
e-mail: dearsanchari@gmail.com

A. Chakraborty
IIEST, Howrah 711103, India
e-mail: angana.chakraborty9@gmail.com

K. Maharatna et al. (eds.), *Computational Advancement in Communication Circuits and Systems*, Lecture Notes in Electrical Engineering 335,
DOI 10.1007/978-81-322-2274-3_31

Conference on Mobile Computing and Networking (MOBICOM'OO), 255–265, 2000), Woungang et al. (Proceedings of IEEE Conference, 2012) and Hu et al. (IEEE J Sel Areas Commun 24(2):307–380, 2006).

Keywords Mobile ad hoc network · Malicious attacks · Reputation

31.1 Introduction

Due to the rapid evolution of wireless network, mobile ad hoc networks (MANETs) are becoming increasingly popular in various applications such as in the field of emergency preparedness and response, collaborative and distributed computing, mine site operations, battlefield military operations, electronic classrooms, conferences etc. [1]. Moreover, MANET becomes popular day by day because it requires no centralized administration or fixed network infrastructure and can be quickly and inexpensively form the set up as needed. In the dynamic MANET environment, nodes are assumed to cooperate among each other to provide routing service and forward packets. This requirement poses a security challenge when malevolent nodes are present in the network. Indeed, the existence of such nodes may not simply disrupt the normal network operations, but also generate severe security problems, like dropping, non-forwarding, authentication, data availability, confidentiality and integrity point of views. In MANETs, reputation-based strategies are considered for detection of selfish/malicious nodes as well as for determining the best forwarder node in case of data delivery. A reputation is a node's degree of cooperation in forwarding and receiving messages.

In this paper, we have done survey and performance analysis on some existing malicious attacks detection and prevention techniques. We have also proposed a model for detection and prevention of malicious attacks using a reputation-based technique. Our proposal is based on personal feedback table maintained by a node for calculating a node's reputation easily. After successful data packet exchange both the communicating nodes will also exchange credit packets; forwarder node will get forward credit from receiver node and receiver node will get receive credit from the forwarder node. Each node will be liable for showing the personal feedback table and credit tables to the Trusted Authority (TA) node for calculating each node's reputation perfectly. TA node is solely responsible for updating reputation values dynamically and broadcast these reputation values and status of a node time to time. After getting these values, a node can easily determine the best forwarder node and selfish/non-cooperative nodes in the network. We have simulated the scheme on Network Simulator (NS2) [2] and compared the performance with [3, 4–6].

The rest of the paper is organized as follows. Section 31.2 presents the related work in this domain. Section 31.3 illustrates our proposed system model. Results and Discussions are included in Sect. 31.4. The paper is concluded with a discussion on future work in Sect. 31.5.

31.2 Related Work

A considerable amount of research has been carried out in the area of MANETs security [7–10]. Some proposed schemes can detect and deal with malicious nodes [11]. The following sections discuss some of the techniques that have been proposed to achieve security in MANETs.

The authors in [12] enhanced the security of DSR protocol by enhancing the trust-based route selection mechanism. The authors in [13] proposed a protocol that calculates the reputation of a node by observing the node's behaviour, the observed value is later altered based on additional observations from other nodes. But node authentication is not mentioned here. In [3] the authors proposed a Trust Scheme for observing the behaviour of mobile nodes. Using this scheme, malicious nodes can be detected and avoided. But which particular node in the route is misbehaving cannot be identified. Node authentication is not used in [3].

In [7] authors proposed a secure Intrusion Detection (EAACK) System for MANETs. In this scheme there are three parts for detection of malicious activities. They are ACK, secure ACK (S-ACK) and misbehaviour report authentication (MRA). It is effective in detecting black hole attacks. Receiver collision problem can be solved. False acknowledgment is not possible.

In [4] authors designed the monitoring scheme to prevent black hole attacks. The solution is that each node in the network consists of two components. One is watchdog and second one is pathrater. Watchdog observes the behaviour of every neighbour by putting itself in promiscuous mode. Pathrater gives the rating of each node in the network. It is possible to detect black hole attack. But false acknowledgement is possible.

The authors in [5] made an intrusion detection-based solution known as anti-black hole mechanism (ABM). In this method, the difference between route request and route reply packets is calculated for every node. This difference between route request and route reply keeps changing due to the forwarding and broadcasting nature of nodes and is stored by every node. But in case of malicious node, difference is high. If the estimated value (difference) goes above threshold value, a block message is broadcasted by the detected node to other nodes to isolate the malicious node. The scheme suffered from high overhead. Node authentication is also not mentioned here.

The authors in [5] recommended a scheme for detecting and avoiding black hole attacks before the actual routing mechanism started by using fake RREQ packets to catch the malicious nodes. These fake RREQ packets are like the normal RREQ but they live only for certain time; fake destination address is used for identifying malicious nodes. But at the time of routing if any node behaves malicious then this mechanism will fail.

In [6] authors proposed a worm hole detection technique. First node is verified and its authorization is done using symmetric key cryptography. If authentication is true, sender can send the data to that particular node; otherwise, next node is selected to carry the data packet. This process continues until data packet reaches to

destination. Here, malicious node cannot pretend to be authorized user. Overhead is huge in this case.

The authors in [14] suggested a method of detecting malicious node during route discovery and if malicious node is found, data packet is sent via another route. This is based on existing protocols like DSR, AODV and DSDV. In this approach encryption techniques, acknowledgement and principles of flow conservation are used to prevent attacks in network layer.

Inspired from these novel works, we have implemented one reputation-based scheme for selfish node detection and avoidance of those selfish nodes in case of further data transmission.

31.3 Proposed System Model

Nowadays, researchers are showing their interest in developing a secured ad hoc network. Many research works are done in detecting the selfish behaviour of node [7, 13]. Motivated from those works, we have implemented one reputation-based selfish node detection scheme based on Ad hoc On demand Distance Vector Routing (AODV) routing protocol. As this selfishness affects tremendously the packet delivery and efficiency of a network, we focused our work on improving the delivery ratio as well as the performance of the overall network.

A node's reputation is determined in terms of its forwarding and receiving characteristics in the recent past by the Trusted Authority (TA) node as in Fig. 31.1. In our proposed model, when a node gets some packet from another node, it needs to maintain one personal feedback table. Suppose, node A is the source of a message and node C is the destination. As node A cannot send the message directly to node C, it needs some intermediate node (here node B) to relay the message to node C which has the higher probability to reach destination node C as in Fig. 31.1. So, A first sends the message to B and updates its personal feedback table as shown in Table 31.1.

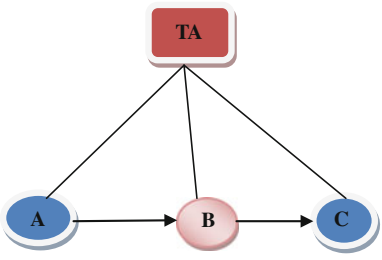

Fig. 31.1 Data exchange from source (A) to destination (C), where B is intermediate node; Trusted Authority (TA) node for calculating each node's reputation

After exchanging messages, node A and node B will exchange credit messages with each other. As node A is the sender so, it will get forward_credit from node B, as well as, node B will get receive_credit by node A. In this scheme, all the messages including data and credit messages are all encrypted messages, encrypted by the owner's private key. So, these messages can be decrypted by any node in the network which knows the public key of node A or node B. So, any node can decrypt the messages, but cannot encrypt it again. In this way, the modifications can be avoided.

From Table 31.1, it is cleared that at time T11, node A had given messages to node B and updated its Personal Feedback table. Here, based on node B's behaviour and previous performance, node A can assign any receive_credit (rc) value of node B up to 1 and node B can assign any forward_credit (fc) value of node A up to 1.

Now, both node A and B can show these credit values or exchange this personal feedback table only to the Trusted Authority for further communication, as reference.

Personal Feedback table maintained by node B is as follows (Table 31.2).

Node B, after getting the message, delivers it to the destination node C. After exchanging messages, node B and node C will exchange credit messages as discussed previously. Based on node C's behaviour and previous performance, node B will assign rc value of node C as 0.7 and node C will also assign fc value of node B as 0.8.

Now, both nodes B and C update their personal feedback tables as shown in Tables 31.3 and 31.4, respectively. We consider T12 > T11.

A sample Forward Credit Table is as shown in Table 31.5.

A sample Receive Credit Table is as shown in Table 31.6.

As shown in Table 31.6, a sample forward credit packet at a particular point of time (say T1) may have fc_id, forwarder node id, receiver node id, number of exchanged packets, exchanged messages' id and exchange time. Similarly, a sample

Table 31.1 Personal feedback table maintained by node A

Source_node id	Forwarder_node id	Time	Forward_credit	Receive_credit
A	B	T11	A-0.9 (by B)	B-0.8 (by A)

Table 31.2 Personal feedback table maintained by node B

Source_node id	Forwarder_node id	Time	Forward_credit	Receive_credit
A	B	T11	A-0.9 (by B)	B-0.8 (by A)

Table 31.3 Updated personal feedback table maintained by node B

Source_node id	Forwarder_node id	Time	Forward_credit	Receive_credit
A	B	T11	A-0.9 (by B)	B-0.8 (by A)
A	C (via B)	T12	B-0.8 (by C)	C-0.7 (by B)

Table 31.4 Personal feedback table maintained by node C

Source_node id	Forwarder_node id	Time	Forward_credit	Receive_credit
A	B	T12	B-0.8 (by C)	C-0.7 (by B)

Table 31.5 Sample forward credit table

Forward credit (fc)_id	Forwarder node id	Receiver node id	No. of exchanged packet	Exchanged msg id	Time
$fc1_{N1}$	A	B	1	M101	T1

Table 31.6 Sample receive credit table

Receive credit (rc)_id	Forwarder node id	Receiver node id	No. of exchanged packet	Exchanged msg id	Time
$rc1_{N2}$	A	B	1	M101	T2

receive credit packet at a particular time (say T2) may have rc_id, forwarder node id, receiver node id, number of exchanged packets, exchanged messages' id and exchange time.

These credit tables are exchanged as a sign of successful completion of data packet exchange. Receiver node will give this to its current forwarder node as a record of how many data packets it receives from current forwarder node and at the same time a forwarder node will give this to its receiver node as a record of how many data packets it forwards to the receiver node (we consider T2 > T1).

Based on forward credit and receive credit, a node will select a forwarder or receiver node but never exchange this personal feedback values to other nodes. So, it definitely reduces overhead.

Each node will also maintain as discussed in Gao et al. [15],

1. Delegation Evidence (D) = {M, A, B, Dst, TS, Exp}-Node A will maintain D.
2. Forwarding History Evidence (F) = {M, B, C, Dst, TS, Exp}-Node B will maintain F.
3. Contact History Evidence (C) = {M, B, C, TS}-Both node B, C will maintain C.

Here M—message, A—node A, B—node B, C—node C, Dst—destination, TS—timestamp and Exp—expiration time of the message.

However, a node will exchange personal feedback table, evidences and credit tables with the Trusted Authority (TA) node for gaining reputation.

31.3.1 Cooperative (Good, Medium) and Non-cooperative/Selfish Node Detection by TA Node

Algorithm1: Cooperative, Non-Cooperative/Selfish Node Detection

```
STEP1: Initialize node under assessment (NA), TA node,
Delegation Evidence (D), Contact History Evidence (C),
Neighbor Table (N), Forwarding History Evidence (F)
STEP2: TA node demands all the nodes in the network to
submit their evidences and Neighbor tables
STEP3: Based on D, C, N; TA node will compare with F val-
ues
STEP4: If F = = Find (D, C, N)
STEP5: NA is cooperative
STEP6: Else
STEP7: NA is non-cooperative or Selfish
STEP8: End if
```

After determining cooperative and non-cooperative/selfish node, TA node will blacklist selfish nodes; but cooperative nodes will go through the reputation process for determining whether the node is good or medium.

Trusted Authority (TA) is the authorized node solely responsible for determining the reputation of a node based on a node's forward credit (fc) and receive credit (rc) values. From the forward credit table and receive credit table, reputation_value at time t is calculated as:

$$\text{Reputation\_value}(t) = \sum \text{fc\_value}(t) \,/\, \sum \text{rc\_value}(t)$$

After getting the reputation of a node, TA node will decide whether that particular node is a good node or medium node.

If reputation_value <= Rth, the node is medium node.

If reputation_value > Rth, the node is good; where Rth = reputation threshold value.

TA node will maintain the reputation table as shown in Table 31.7.

From Table 31.7 it is cleared that TA node maintains the reputation table and reputation values with timestamp for each node and periodically updates this table.

TA node will broadcast this reputation table time to time so that all other nodes in the network can choose best forwarder node for data delivery.

Here also, selfish nodes will get another chance to gain their reputation. If any node fails to increase its reputation even after getting second chance, it will be temporarily avoided from future communication to improve packet delivery.

Table 31.7 Sample reputation table maintained by TA node

	N_1	N_2	…	N_i	…	N_j
TA	$R1_{t0}$	$R2_{t2}$	…	Rj_{tj}	…	Rk_{tk}

31.4 Results and Discussions

31.4.1 Simulation Details

We have implemented our scheme using Network Simulator (NS2) [2]. We have also made the comparison with other schemes discussed in the papers [3, 4–6]. The details of the simulation parameters are discussed in Table 31.8.

The performance of our proposed scheme and other schemes are evaluated in terms of packet delivery probability and routing overhead.

Delivery Probability: Delivery Probability defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

Routing overhead: Routing overhead defines below formula

$$\text{Routing overhead} = \frac{(\text{No. of packets relayed} - \text{No. of packets delivered})}{\text{No. of packets delivered}}$$

31.4.2 Discussion About the Output

We have done our simulation on a basic packet dropping attack. Malicious nodes simply drop all the packets that they receive. We considered two scenarios.

In scenario 1, we have observed delivery probability in Fig. 31.2 where malicious nodes are varied from 0 to 40 %.

In scenario 2, we have observed routing overhead in Fig. 31.3 where malicious nodes are varied from 0 to 40 %.

We have compared the performance of our proposed scheme with

(i) Malicious nodes detection scheme discussed in paper [3]
(ii) Mitigating misbehaviour scheme discussed in paper [4]
(iii) Prevention of black hole scheme discussed in paper [5]
(iv) Wormhole attacks detection scheme discussed in paper [6].

Table 31.8 Parameters used

No of nodes	100
Terrain range	1000 × 1000 m^2
Speed of mobile node	0, 5, 10, 15, 20 m/s
Pause time	300 s
Packet size	512 Bytes
Simulation time	3,000 s
Packet transmission rate	4 packets/s
Routing protocol	Ad hoc on demand distance vector (AODV) routing

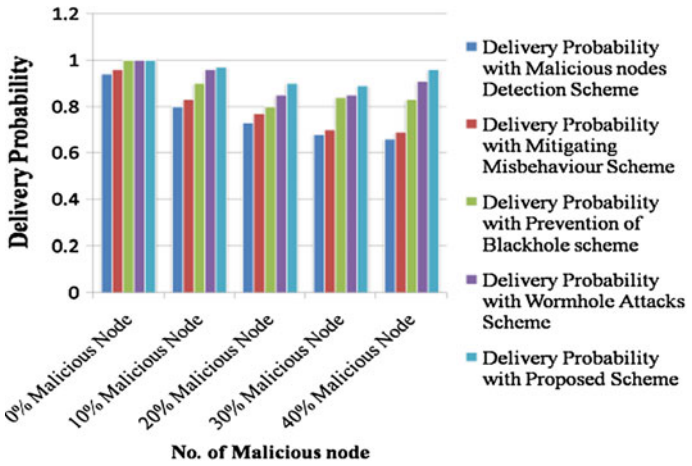

Fig. 31.2 Simulation result of delivery probability where malicious nodes are varied from 0 to 40 %

From Fig. 31.2, it is cleared that using our proposed scheme maximum delivery probability can be achieved compared to other schemes.

We can easily notice from Fig. 31.3, that in our proposed scheme routing overhead is minimum compared to other schemes.

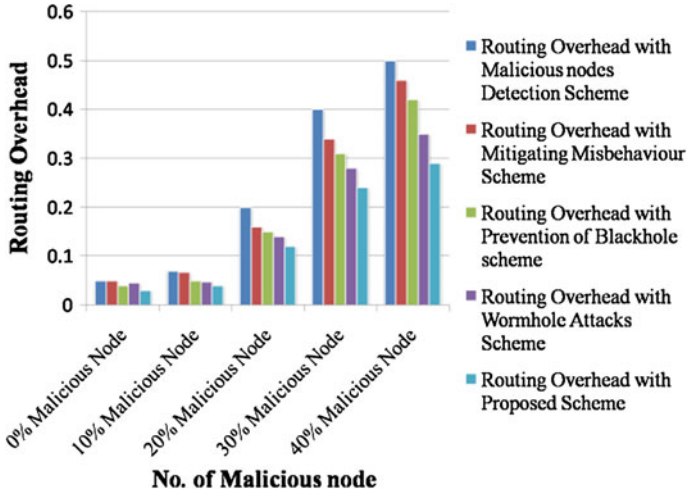

Fig. 31.3 Simulation result of routing overhead where malicious nodes are varied from 0 to 40 %

31.5 Conclusions and Future Work

This paper presents a reputation-based scheme for selfish node detection and avoidance of those selfish nodes in case of further data transmission in mobile ad hoc network (MANET).

The uniqueness of our reputation estimation scheme is that

(i) It is distributed and dynamic in nature, i.e. nodes with a bad reputation may get further opportunity to improve their reputation by participating and cooperating in future data communication.
(ii) Our proposed system ensures data integrity as every data packets are sent using public key cryptosystem and other personal feedback tables, credit tables and reputation tables are sent after digitally signed by the source node.

In this paper, we can easily detect the malicious activities like dropping, non-forwarding, false token generation, colluding attacks and we have made efforts to avoid those nodes during data forwarding. We have evaluated the performance in terms of delivery probability and routing overhead. However, the impact of mobility and scalability is not evaluated yet, which is included in our future work.

References

1. P. Michiardi, R. Molva, CORE: A Collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in *Proceedings of IFIP-Communication and Multimedia Security Conference* (2002)
2. NS2 simulation package, http://www.isi.edu/nsnam/ns/
3. Y. Khamayseh, R. Al-Salah, M.B. Yassein, Malicious nodes detection in MANETs: behavioral analysis approach. J. Netw. **7**(1), 116–125 (2012)
4. S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in *Proceedings of International Conference on Mobile Computing and Networking* (*MOBICOM'OO*) (2000), pp. 255–265
5. I. Woungang, S.K. Dhurandher, R.D. Peddi, M.S. Obaidat, Detecting blackhole attacks on DSR-based mobile ad hoc networks, in *Proceedings of IEEE Conference* (2012)
6. Y.-C. Hu, A. Perrig, D. Johnson, Wormhole attacks in wireless networks. IEEE J. Sel. Areas Commun. **24**(2), 370–380 (2006)
7. E.M. Shakshuki, N. Kang, T.R. Sheltami, EAACK—a secure intrusion-detection system for MANETs. IEEE Trans. Ind. Electron. **60**(3), 1089–1098 (2013)
8. J.W. Huang, I. Woungang, H.C. Chao, M.S. Obaidat, T.Y. Chi, S.K. Dhurandher, Multi-path trust-based secure AOMDV routing in ad hoc networks, in *Proceeedings of IEEE Globecom* (2011), pp. 1–5
9. C. Chakrabarti, R. Chaki, Improved cluster based route discovery algorithm for ad-hoc networks, in *Proceedings of IEEE ICCIA* (2011), pp. 1–4
10. C. Chakrabarti, A. Banerjee, S. Roy, An observer-based distributed scheme for selfish-node detection in a post-disaster communication environment using delay tolerant network, in *Proceedings of IEEE AIMoC* (2014), pp. 151–156
11. A. Nadeem, M.P. Howarth, A survey of MANET intrusion detection and prevention approaches for network layer attacks. IEEE Commun. Surv. Tutorials **15**(4), 2027–2045 (2013)

12. M. Alsaadi, Y. Qian, Performance study of a secure routing protocol in wireless mobile ad hoc networks, in *2nd International Symposium on Wireless Pervasive Computing* (IEEE Computer Society, New York, 2007), pp. 425–430
13. G. Bella, G. Costantino, S. Riccobene, Evaluating the device reputation through full observation in MANETs, J. Inf. Assur. Secur. **4**, 458–465 (2009)
14. S. Arya, C. Arya, Malicious nodes detection in mobile ad hoc networks, J. Inf. Oper. Manag. **3** (1), 210–221 (2012) ISSN: 0976–7754 & E-ISSN: 0976–7762
15. Z. Gao, H. Zhu, S. Du, C. Xiao , R. Lu, PMDS: a probabilistic misbehavior detection scheme in DTN, in *IEEE ICC 2012—Wireless Networks Symposium* (2012)