I.J. Wireless and Microwave Technologies, **2017, 4, 28-37**
Published Online July 2017 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2017.04.03

***Available online at** http://www.mecs-press.net/ijwmt*

An Enhanced Reputation-based for Detecting Misbehaving Nodes in MANET

Mohammed Azza, Sofiane Boukli Hacene[a,b]

[a,b]*Department of Computer science, Djillali Liabes University of Sidi Bel Abbes, Algeria*
Evolutionary Engineering and Distributed Information Systems Laboratory, EEDIS.

Abstract

In this paper, we propose an enhanced approach based on first-hand reputation with allows to detected misbehavior node in Manet. The network's security is an important challenge in this kind of networks. The main objective of the misbehaving nodes in AODV routing protocol deletes all data packets that received thus, don't transmit to their destination. In a reputation-based system, each node overhears the activity of its neighbors (transmit and receive) in first-hand or combined with second-hand. Our approach is composed of three-phase directly monitoring, calculating reputation value and node isolation. The reputation value is enhanced by the packet dropped due to other events such as overloading of queue and node availability. The node with a negative reputation will be isolated, and an alert packet will be distributed to neighboring nodes to inform, afterwards an improved local repair is started. The simulation results show that the proposed approach can detect and isolate a malicious node, which improves the packet delivery ratio and lowest increasing in the throughput, while reducing the success rate of the misbehaving nodes.

Index Terms: MANET, AODV, Misbehavior, reputation-based, Monitoring, NS2.

1. Introduction

MANET Mobile Ad hoc Networks are developed due to their vast use. They are composed of a group of mobile units that move in a free and quickly way. In these kinds of network, there is no infrastructure and no centralized unit where the mobile units are responsible for establishing and maintaining network connectivity with a continuous way. MANET is actually easier to deploy in difficult situations. It is used first time in the military domain [1].

MANETs are multi-hop environments [2] that each unit will participate in the routing process for

* Corresponding author.
E-mail address: azza.mohammed.amine@gmail.com

constructing a path toward the destination, the entire unit selected in the path must cooperate for transmit the packets to the destination. This collaboration makes the network vulnerable to many types of attacks.

The established a path to the destination we need a routing protocol such as AODV; it's a reactive routing protocol where each intermediate node cooperates in the routing process.

The attacks are classified into several categories active and passive [3]; the attacker in black hole disrupts the functioning of the network with false response information RREP and does not participate in the relay of route request packets RREQ. Afterwards, it removes all data packets that receive[4].

Literature gave us many approaches to preventing them malicious nodes such as reputation-based (RB) and credit-based (CB) [5]. Reputation is the value that reflects the collaboration of a node if a node cooperates maximally so its reputation is highest against a node that does not cooperate where his reputation is lowest [6]. The reputation can be calculated by central node or specific node or distributed where each node calculates the reputation of its neighbors. We distingue two kinds reputation-based overhearing and reputation-based acknowledge [7].

The rest of the paper is organized as follows: In section 2 we define the networks model and some notations used in this paper, after in section 3 we describe some approach was already proposed. We explain in section 4 our approach and its evaluation with some parameter through a simulation with NS2 described in section 5. Finally, we conclude in section 6 with a future scope.

2. Networks model and Notation

2.1. Networks model:

A MANET is modeled as a directed graph DG(N,E), where $N = N_1; N_2; \ldots; N_k$ represents the set of K mobile nodes and E represent the communication links between a pair of nodes in the same transmission range. The reputation value of node N_j as perceived in node N_i as represented by R_{ij} values. We suppose a bidirectional communication in each communication link. All notations used in this paper are summarized in Table 1.

Table. 1. Notation used in our approach

Notation	Description
NGSi	Set of neighbors node of Ni
N	Node Ns,..,Ni, Nj,..Nd where Ns is source and Nd is the destination
PNTj	the number of packet transmitted by Ni and not relayed by Nj.
PSNj	the number of packets transferred by Nj
PERj	packets dropped a cause overload of queue or broken link of Nj.
RECVj	the number of packets receives in Nj.
Rij	Reputation of Nj maintained by Ni
Rt	Time of calculating the reputation
Rexp	Time of expiration of reputation
Rinit	started reputation

2.2. Misbehavior node:

The lake of a central unit in MANET makes this vulnerable for many attacks, in general, there are two categories of attack: passive and active attack [8]. The malicious node with passive attacks gets traffic information without authorization such as listening. In active attacks, the attacker disrupts the routing process. It transmits false information to violate the data transmitted or the exhaustion of network resources such as

energy. In our study, we define a malicious behavior node, each node that cooperates in the route discovery process with the best path to the destination. The objective of this node is taken part of the active data transmission link. The malicious node can act with the following actions [9, 10]: Removing RREQ packets, For each RREQ received the malicious response with an RREP packet that contains a larger values of the sequence number and the malicious nodes delete all the data.

2.3. AODV Routing Protocol

AODV is a distance vector routing algorithm designed by Charles E. Perkins and Elizabeth M. Royer[11] . It is a reactive routing protocol used in situation where there is a frequented change in networks. Due to mobility nodes become unreachable. To establish a new route toward destination becomes necessary. AODV uses the sequence number as information to describe the freshness of route. AODV is composed of two-Phase route discovery and route maintenance.

3. Related Works

Many interesting mechanisms have been studied and developed to address various reputation-based systems in Ad Hoc networks. The main idea of the system of reputation is that each node monitors the activity of its neighbors (transmitter and receiver mode). This system is composed of three main phase: monitoring, reputation management and isolation.

A normal node cooperates in the communication processes so his reputation has a maximum value against node misbehavior that has a low value [10]. The value of reputation calculates are compared with threshold values for determinate a malicious node, and updated in each interval of times [12]. There is a reputation management system that uses both first-hand and second-hand information for updating reputation values. The first one obtained directly by the monitoring phase, and de second defused by neighbor node [13]. Some of the efficient approaches are enumerated below. Authors in [14] define an approach for make a Reputation System in Ad Hoc networks named OCEAN (Observation-based Cooperation Enforcement in Ad Hoc Networks). This method based on first-hand observation of neighbor communication. OCEAN solves the problem of vulnerable reputation exchanged by neighbor (second-hand) and gives second chance for malicious node to prove their reliability.

CONFIDENT: (cooperation of nodes: fairness in dynamic ad hoc networks) are proposed by [15]. It is a hybrid system based on the trust developed in DSR routing protocol for detect and remove the malicious node. It composes to four components are the monitor, the reputation manager, the path manager and he trust manager. Authors in [16] proposed a reputation-based technique that employs which a watchdog and path rater. The Watchdog overheard the packets forwarded by next hop, afterward it compared witch de same packets in the buffer. If there is a match, the packet is removed from the buffer, and the node is determined as a normal node. A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks proposed by Michiardi and Molva [17]. CORE employs three kinds of reputation (subjective, indirect and functional). The final reputation is estimated by combining different weights of different functional reputation. Authors in [18] distributed a message for evaluated the reputation and reliability of a node in the network. The reputation of the nodes is based on the quality of service in the reception of packets, and reliability is based upon the feedback after every successful transmission. Ankit and al in [19] proposed a method that combines the route discovery phase and the data transmission phase to detect the malicious node. In route discovery phase, if the sequence number of destination exceed a threshold value then the RREP is rejected. Afterward during the data transmission phase, the node calculates the difference between transmitted and received packets. If this difference exceeds a threshold value then the node is malicious. The identities of malicious node are distributed to neighbors' node and a blacklist is maintained.

4. Proposed solution

When we compared some related works above our proposed model, an important difference is in the monitoring technology that uses in the detection of misbehaving nodes. Most techniques used Monitor watchdog, it overhears the packets transmitted, received and discarded to calculate the corresponding values of reputation. This method has its own limitations. In the MANET, the transmission is apt to many occurrences as packet collisions, the queue overloading and inaccessibility of destination by their movement or energy exhaustion; all this can tack to an erroneous detection.

In our proposed work, we have enhanced the monitoring phase, it's not based only on data transmit (send and receive) for calculate the reputation of its neighbors. But all the circumstances of the node will be taken account such as overloading of the queue, broken of link and exhaustion of energy. The objective of our proposal is to identify and isolate the malicious node, why our process consists of three phases: (Monitoring, Computes reputation and Isolation and route maintenance)

4.1. Monitor or surveillance:

It is the phase responsible for the direct observation of each neighbor node N_j where N_j belongs in NGS_i. Each node overhears the forwarded and receiver data packets of their neighbor.

We adapt to our monitoring a solution where the node waits for a time slot to hear if the packet is forwarded to the next hop. If the packet is transmitted, node's reputation is increased; otherwise, node's reputation is decreased. The reputation is recalculated periodically, using the equation 1.

The collaboration of the neighboring node CL_j is calculated by the number of data packet transmitted in relation to the number received. The misbehaving node removes all the packets received and does not transmit to their neighboring nodes. But, there are different conditions that the packets were deleted such as overloading of the queue or path failure that relay to the next hop.

In our method, we added for consistency the congestion and unreachable of the next hop, if the number of retransmission reaches the max "MAC_RETRY_COUNT_EXCEEDED", so the packet is removed due to overloading of the queue by mac layer. The node tells the callback to send a failed operation to up layer with the variable "xmit_failure_data_". In this case we added for calculate the reputation the error packet (RERR) that influence in the reputation of node.

To distingue between overloading of the queue and unreachable of the node we added in the packets CTS two information's a residual energy field and the status overloading of the queue.

4.2. Reputation System:

In our approach, we calculate a reputation value R_{ij} by node N_i for node N_j about of data transmits. We used to determine the malicious nodes a set of counters for each neighbor node $N_j \in NGS_i$. When the number of packets receives in N_j achieve a threshold values P_j, in this case, we can judge their behavior.

The R_{ij} is a real number; a positive value indicates that the node is cooperative while a negative value or nil indicates that the node is misbehaving. The reputation of a node is maintained by his neighbors until a period of time R_{exp}. The set of counters are updated as the following rules:

- Rule 1; for each packet received in N_j and relayed the PSN_j is incremented by one.
- Rule 2; for each packet received in N_j and not relayed the PNT_j is incremented by one.
- Rule 3; for each packet received at N_j and not relayed due to overloading of queue or broking of the link the PER_j is incremented by one.

Given PNT_j PSN_j PER_j we calculate the reputation of neighbor node N_j in time R_t.

$$R_{ij} = Cl_j - PNF$$
$$R_{ij} = \left(\frac{PSN_j}{RECV_j} + \frac{PER_j}{RECV_j} \right) - \left(\frac{PNT_j}{RECV_j} \right) \quad (1)$$

Where PNF represent the ratio of packets not relayed it reflects the bad cooperation of node.

After expiry time each node updates the reputation of its neighbors according to equation 2. The node that joints the network is assigned a neutral reputation R_{init}.

$$R_{ij}^{t} = \alpha \times R_{ij}^{t-1} + (1-\alpha) \times R_{ij}^{t} \quad (2)$$

We define $\alpha = 0.4$ to give more chance for malicious node to improves his reputation and $P_j = 3$ packets. Algorithm 1 summarized the reputation phase.

4.3. Isolation and route maintenance:

If a malicious node is detected witch reputation phase, it calls an isolation process. The node stops transmission of all packets passing through this misbehavior. Afterward, he adds this malicious node in black list and informs all neighbors with a packet control "Alert". If all neighbors were averted a local repair are

```
BEGIN
FOR each data packets send by Ni and received at Nj do
        IF Nj = = Nd THEN
                Send DATA
        ELSE
                Send DATA
                Update RECVij
        END
        IF RECVij < Pj THEN
                IF Nj transmit DATA
                        Update PSNj according rule 1
                ELSE
        IF   Nj send RERR to Ni
                Update PERj according rule 3
        ELSE
                UPDATE  PNTj according rule 2
                Packets is dropped
        END IF
END IF
ELSE
        Compute Rij  according equation (1)
        IF Rij < 0 and THEN
                Node is malicious
                Call Isolation phase
        ELSE
                Continue la transmission
        END IF
END IF
END FOR
END
```

Algorithm 2 : reputation phase

```
BEGIN
  IF Nj in Black_list THEN
        IF Counter > Th
          Set Texp =infinity
        ELSE
          Set Texp =time slot
        END IF
  ELSE
        Add Nj to Blacklist
        Set Texp =time slot
        Counter=1
  END IF
        Stop data transmission
        Buffered DATA
        Send Alert to neighbors
        Route repair
END
```

Algorithm 2 : isolation phase

started otherwise a global repair. If the counter is more than a threshold values it means that the node is detected more than once, in this case the node will never be removed from Black_list. In route maintenance we enhanced the reparation of route with two information's a residual energy and the state of overloading of the queue. We choose the next hop with a maximum residual energy and low overloading of the queue. The algorithm 2 illustrates the functioning of this phase.

5. Simulation and Performance Evaluation

We use Network Simulator (NS2.35) to simulate the proposed method. Our simulation parameters and parameters are summarized in Table 2. The evaluation was done by analyzing results of three conditions (AODV protocol, AODV protocol with node misbehavior and our approach with node misbehaviour

Table. 2. Parameter of simulation

PARAMETER	VALUES
Number of Node	51
The Traffic Types	CBR
Mac layer	802.11
The Packet Size	512 Octets
Send Frequency	4 Packets/Second
Speed Maximum	10 M/S
Time of Simulation	200 S
Size of Topology	800 X 800 M

We are using tree parameters to simulate our approach: Packet Delivery Ratio (PDR) , The average latency of data packets (Delay) and Additive costs (overhead)

5.1. Discussion

Packet Delivery Ratio (PDR): The Figure 1 illustrates the evolution of the Packet Delivery Ratio (PDR) with misbehavior node, without misbehavior node and our proposition with misbehavior node. The observation of this figure illustrates that the PDR of our approach is better than protocol with misbehavior node, this justifies that the detection and isolation by reputation-based work well. In pause time = 0 the degradation of the PDR is 20,21% in our proposition. When a pause time increased the nodes are very stable which will the PDR reduces lightly to 3,65% in our approach against a normal protocol. The degradation of the PDR with misbehavior is proved by the number of packets transmitted is considerably higher than the number of packets received. The number of packets sent is important because all data packets received by the misbehavior node are generally dropped. We see that the PDR under attack decreases 90,91% against to protocol without attack.

Traffic Control: The observation of the figure 2 shows an evolution increasing of traffic control based on Pause time. We note that the protocol AODV under attack generates less control traffic than standard protocol AODV, This is due because the malicious node observes the RREQ packets and does not rebroadcast as there is a high probability of ruptures of links in Pause time =0. As a measure to the network stabilize (pause time = 200) the control packets decreasing. Our approach produces more control traffic against the protocol normal it justified that our method generates other control packet alert, this packet used to inform the neighbor's node about the misbehavior node.

The Average Latency Of Data Packets (Delay): The figure 3 shows the result of end-to-end delay depending a pause time. We observe that, the delay is affected by the reputation-based system at (pause time = 0) because the data packets are buffered in detection of the misbehavior node until the local repair started. The

results show that the end-to-end delay of our proposed is higher than those of AODV and AODV with attack, because the nodes are forced to rebuild the invalid paths. When the network stabilizes (pause time = 200) the delay decreased, for a reason that our approach established a provided route to avoid a malicious node through the reputation-based technique. So it is found that the time required to our approach is higher than AODV and AODV under attack.

The effect of α and P_j in success rate of misbehavior node: In this experiment, the malicious drop ratio was obtained across varying in the values of α. We observe in figure 4(a) that, if the α value increase as the success rate of node misbehavior increases where $\alpha \geq 0{,}4$. In addition where $\alpha=0$ the success rate is smaller, this means that the reputation value of the node is based only on the recent value calculated according to rule (2). When $\alpha=1$, in this case, the reputation value negative and the success rate is higher although that the node has changed its reputation.

In figure 4(b), we observe that if the value of P_j increase the success rate of misbehavior increase because P_j represents the number of packets that receive before judging the behavioral of the node.

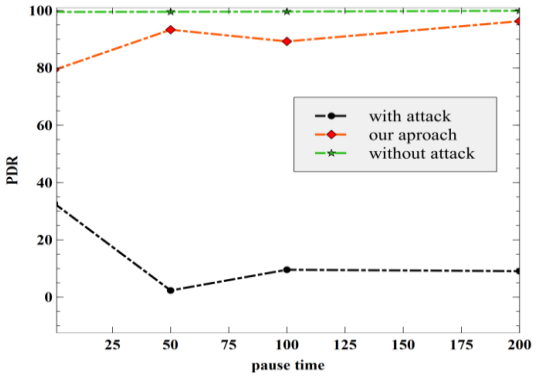

Fig.1. Effect of pause time in PDR

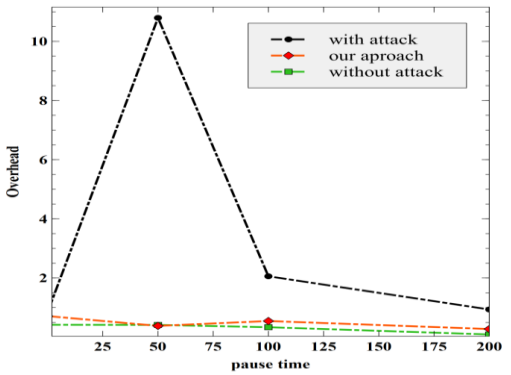

Fig.2. Effect of pause time in overhead

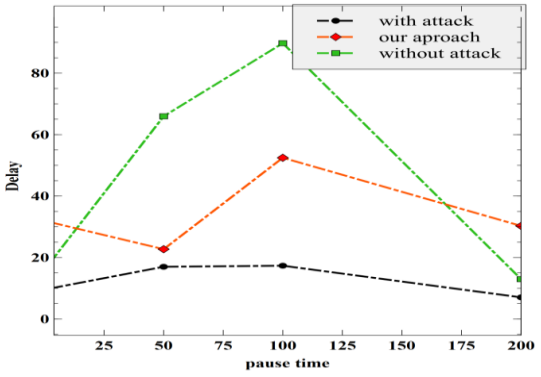

Fig.3. Effect of the pause time in delay

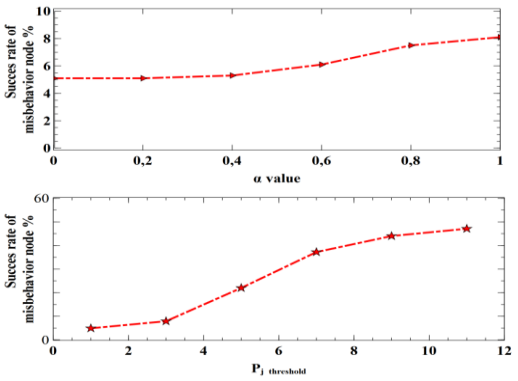

Fig.4. a The effect of α. b The effect of P_j

6. Conclusions

In this article, we have proposed an enhanced reputation-based method to detect and isolate the misbehavior node in mobile ad hoc networks. Our approach composed of three phases. Firstly, the monitoring phase is defined by the directly overhearing of packets send and receives (first-hand). If the number of packets received in next hop equal to a threshold value, currently we can be judged this node. Secondly, the calculations of reputation are enhanced by the error packets generated due to overloading of queue and the unavailability of next hops, this information can be distinct to dropped packets with the misbehavior node and other events. The node with a negative reputation was isolated and the routes that include this misbehavior are repaired. The route repair takes account another QoS parameter such as degree of overloading of queue and the energy residual to establish a new route.

In our future work, we plan to enable nodes to exchange their reputation and take account different parameters in calculating of reputation values.

References

[1] Kannhavong, B., et al., A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, 2007. 14(5): p. 85-91.

[2] Junhai, L., et al., A survey of multicast routing protocols for mobile ad-hoc networks. IEEE communications surveys & tutorials, 2009. 11(1): p. 78-91.
[3] Kumar, J., M. Kulkarni, and D. Gupta, Effect of Black hole Attack on MANET routing protocols. International Journal of Computer Network and Information Security, 2013. 5(5): p. 64.
[4] Bibhu, V., et al., Performance Analysis of black hole attack in VANET. International Journal Of Computer Network and Information Security, 2012. 4(11): p. 47.
[5] Subramaniyan, S., W. Johnson, and K. Subramaniyan, A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique. EURASIP Journal on Wireless Communications and Networking, 2014. 2014(1): p.1
[6] Liu, J. and V. Issarny. Enhanced reputation mechanism for mobile ad hoc networks. in International Conference on Trust Management. 2004. Springer.
[7] Liu, K., et al., An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE transactions on Mobile Computing, 2007. 6(5): p. 536-550.
[8] Joseph, C., et al., Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios. Indian Journal of Science and Technology, 2015. 8(29).
[9] Dini, G. and A.L. Duca, Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network. Ad Hoc Networks, 2012. 10(7): p. 1167-1178.
[10] Akhtar, A.K. and G. Sahoo, Classification of Selfish and Regular Nodes Based on Reputation Values in MANET Using Adaptive Decision Boundary. Communications and Network, 2013. Vol.05No.03: p. 7.
[11] Perkins, C., E. Belding-Royer, and S. Das, Ad hoc on-demand distance vector (AODV) routing. 2003.
[12] Wang, F., et al., COSR: a reputation-based secure route protocol in MANET. EURASIP J. Wirel. Commun. Netw., 2010. 2010: p. 1-13.
[13] Han, G., et al., Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences, 2014. 80(3): p. 602-617.
[14] Bansal, S. and M. Baker, Observation-based cooperation enforcement in ad hoc networks. arXiv preprint cs/0307012, 2003.
[15] Buchegger, S. and J.-Y. Le Boudec. Performance analysis of the CONFIDANT protocol. in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. 2002. ACM.
[16] Marti, S., et al. Mitigating routing misbehavior in mobile ad hoc networks. in Proceedings of the 6th annual international conference on Mobile computing and networking. 2000. ACM.
[17] Michiardi, P. and R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in Advanced communications and multimedia security. 2002, Springer. p. 107-121.
[18] Ayday, E. and F. Fekri. BP-P2P: Belief propagation-based trust and reputation management for P2P networks. in Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society Conference on. 2012. IEEE.
[19] Patel, A.D. and R.H. Jhaveri, Addressing Packet Forwarding Misbehavior with Two Phase Security Scheme for AODV-based MANETs. International Journal of Computer Network & Information Security, 2016. 8(5).

Authors' Profiles

Mohammed AZZA received M.Sc in computer science departement from Djilali Liabes University. He is pursuing PhD in Computer Science and Engineering from Djilali Liabes University. His main research area includes Mobile Ad hoc Networks, Wireless Sensor Network. His subjects of interest include Analysis of Cryptographic Protocols, Network Security and Information Security. He is a life member of EEDIS laboratory.

Sofiane BOUKLI HACENE Associated Professor at Computer Science Department of the Djillali Liabes University (U.D.L) of Sidi Bel Abbes (Algeria). He received an Engineering degree (first class honors) from U.D.L in 2002, the M.S. degree from Al Al Bayt University at Mafraq (Jordan) in 2005, PhD from U.D.L in 2012 and the habilitation to supervise research (HDR) in 2014. He is a head of "Evolutionary Engineering and Distributed Information Systems laboratory" at the U.D.L. His research interests are in networking, including wireless ad-hoc, sensor network, vehicular network and network security.

How to cite this paper: Mohammed Azza, Sofiane Boukli Hacene,"An Enhanced Reputation-based for Detecting Misbehaving Nodes in MANET", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.4, pp.28-37, 2017.DOI: 10.5815/ijwmt.2017.04.03