International Journal of Soft Computing 11 (7): 492-496, 2016
ISSN: 1816-9503

Direct and Indirect Approach Based Reputation Scheme Framework for Detecting Blackhole Attacks in Manets

[1]V. Geetha and [2]Hari Prasad
[1]Department of ISE, R.V. Collage of Engineering, 59 Bangalore, India
[2]Jain University, Bangalore, India

Abstract: Security attacks in MANETs can happen in any layer of the protocol stack. The attack can be a active attack or passive attack. In network layer attack by misbehaving nodes called "malicious nodes" can disrupt the proper functioning of the underlying routing protocol by corrupting the routing information in terms of tailoring false routing information or "impersonating other nodes". Few malicious node attack patterns are Blackhole attack wormhole attack or tunnelling, grayhole attack etc. In this study, we have proposed a direct and indirect approach based reputation scheme framework for detecting blackhole attacks in MANETS. But this proposed framework improvises the AODV protocol towards achieving the goal of detecting the malicious nodes attack in MANETS. Thus, improving the performance of reputation approach is shown and analysed using the throughput as a metric in this study.

Key words: AODV (Ad-hoc On Demand Vector), blackhole, reputation based model, direct indirect approach, India

INTRODUCTION

Blackhole attack is one of the malicious nodes attack pattern. In blackhole attack the attacker node advertises itself for posessing shortest path to the destination. It uses its routing protocol in order to pose the zero metric for all destinations irrespective of routing table entry, hence causing routing of packets towards it. Thus in protocol like AODV which are based on flooding technique, the malicious node's forged reply messages will be received before the reply messages from the original destination/actual node. A fake route is hence created and established, leading to packet drop or packet forward to the unknown address. The blackhole attacks are severe and affects the whole network which leads to the demand of efficient security framework for detecting the blackhole.

Detection and prevention of malicious node attacks in manets: There are various approaches ranging from simple to complex for detecting and preventing the attacks in MANETs like: watchdog, random feedback, reputation based, mobile intrusion detection system, currency rewarding system etc. Few techniques are very simple but others are powerful and also apply intelligence to identify and punish misbehaving nodes in the network.

Our proposed framework is based on reputation scheme detects malicious nodes blackhole in high mobility scenario of MANET's. The performance efficiency of the framework is analyzed in the presence and absence of blackhole nodes in the network using the plain AODV and improved AODV as the routing protocol.

MATERIALS AND METHODS

Motivation for choosing reputation based scheme: Many other schemes helps us to detect the blackhole attack such as credit based scheme, watchdog scheme incentive based scheme etc. The motivation and the reason to choose reputation based scheme is its unique feature, i.e., If a node successfully contributes in the transmission of data by forwarding data packets, the reputation of the node is increased, or if the node discards the packet by dropping it, the reputation is decreased and if a node successfully contributes in the transmission of data by forwarding data packets, the reputation of the node is increase or if the node discards the packet by dropping it, the reputation is decreased. When comparing with the other approaches such as credit based scheme detects only selfish nodes and Tamper-proof hardware to monitor the increase or decrease of the virtual currency is required. Where as watchdog is responsible for neighbor monitoring and identifying malicious and selfish nodes whereas pathrater module evaluates the overall reputation of nodes and defines route by excluding the selfish or misbehaving nodes and It can't detect the selfish nodes

Corresponding Author: Geetha, Department of ISE, R. V. Collage of Engineering, 59 Bangalore, India

in case of limited transmission power, ambiguous collision, receiver collision, minor dropping etc. In 2ACK (two-way acknowledgement) scheme nodes explicitly send acknowledgement two hops upstream to verify cooperation and is susceptible to collusion of two or more consecutive nodes (Cho *et al*., 2010).

Comparative study of existing reputation mechanisms: Under the category of reputation based scheme there are several schemes to detect the malicious nodes such as CONFIDANT (Cooperation of Nodes, Fairness In Dynamic Ad-hoc NeTworks), CORE (Co-operation Enforcement based on reputation), OCEAN (Observation based Cooperation Enforcement in Ad Hoc Networks), SORI (Secure and Objective Reputation-based Incentive Scheme) are surveyed.

CONFIDANT uses both direct and indirect approach to detect only malicious nodes. And the malicious nodes are isolated and trusted Recommendations are taken into Account. But observation is based on passive ack. Does not detect selfish nodes using DSR protocol (Buchegger and Boudec, 2002).

CORE uses both direct and indirect approach to detect only selfish nodes and second chance is given for nodes in bad locations and no negative ratings are communicated. But dependence on passive ack, more weight is given to past behavior and hence recent misbehavior will be ignored using DSR protocol (Mahmoud *et al*., 2005).

Does not detect malicious nodes. OCEAN uses only direct approach to detect both selfish nodes and malicious nodes and no punishment strategy is accompolished. Ocean will distinguish the selfish and misleading nodes, it maintains overall network throughput with existence of selfish nodes at network layer.but it It fails to punish the misbehaving nodes severely using DSR protocol (Bansal and Baker, 2003).

Need for the framework: There exists a need of framework comprising:

- Algorithm for detecting and classifying selfish and malicious nodes
- Algorithm for incorporating the direct and indirect reputation based approach
- Mechanism for inculcating the punishment strategy for the badly reputed nodes
- Second hand scheme for badly reputed nodes to participate in the routing process again

This study includes only the malicious nodes in the framework for AODV protocol. Future enhancement of the work will include selfish nodes as well as the punishment strategy and second hand scheme for the badly reputed nodes. Thus from the need for the Framework first two needs are satisfied and analysed in this study.

Proposed reputation scheme framework for detecting and preventing blackhole attacks: Reputation model is a useful tool for facilitating the decision making in MANETs. Reputation is the opinion of one node about the other in the wireless network and signifies the trustworthiness of one node. Reputation model can cope with any kind of node misbehaviour thus is an effective way to handle selfish behaviour and malicious behaviour in the network. Reputation based framework enable nodes in MANETs to make informed decisions about their prospective transaction nodes in the network (Fig. 1).

Data structures used: Let aR (i,j) and aT (i,j) be the reputation rating and trust value respectively that node i has about node j. Every node has these data in the reputation table maintained individually. The node also has a data stucture aF (i,j) which is the node j information that node i stores through its direct observation, i.e., direct approach. Blacklist (k) a list of black listed nodes (Buchegger *et al*., 2008).

Proposed framework phases

Bootstrapping phase: All nodes in the network are considered untrustworthy and are initialized with negative (-1) trust value. aT(i,j) is initialized to-1, aR(i,j) to "not defined" and aF (i,j) NULL. When the node reputation is increased because of its good encounters, then the trust value is increased.

Initialization phase: All the nodes in the network are considered trustworthy and hence assign maximum trust value to each pair of the nodes is entered in reputation table. aT (i,j) is initialized to MAX , aR (i,j) to "GOOD" and aF (i,j) to NULL. The trust value reputation of the node may decrease with its every bad reputation .

Information gathering phase: Gather the information of the intended node based on the direct and indirect information. Watchdog is used to monitor the nodes behaviour and report its observations. The data structures aF (i,j) is filled for the node pair with the direct observation information. Indirect information is restricted to only context aware negative information collection which helps to reduce the node's reputation based on its bad reputation.

A node is labelled malicious if and only if its negative behaviour is reported indirectly by more than four nodes

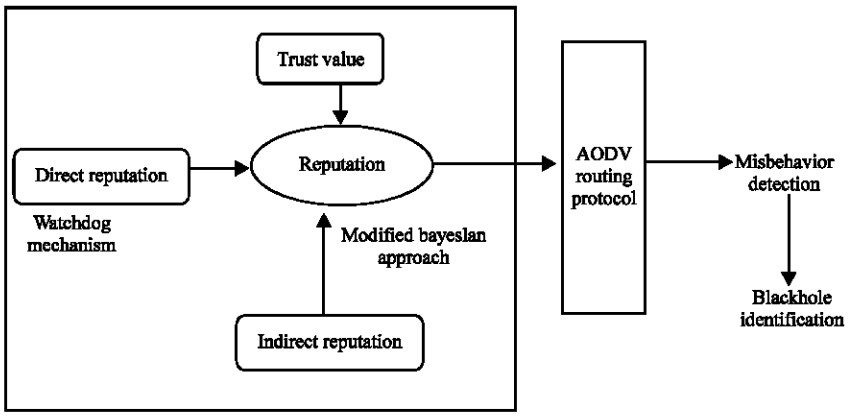

Fig. 1: Architectural design

in the neighbourhood. Else the information reporting node itself is considered as malicious and its reputation is updated suitably and the node is listed in the blacklist. With the information gathered by the above said means, the trust value for the intended node for the reputation table is computed and is updated.

Information sharing phase: The proposed model use proactive dissemination method to communicate the reputation information in the network at each dissemination interval. At the last dissemination interval the node publishes the reputation values irrespective of changes happened or not. This strategy is selected as it is suitable for dense network with more activities. The model also implements global locality of information dissemination using multicasting technique which propagates the information to nodes outside the range of the node who is publishing the reputation information. This is beneficial for higher mobility network as it provides nodes with reasonable understanding of new locations they are moving to.

The node publish its aF(k, j) information to nodes in its communication range., say a node i receives from node k the direct observation information of node j. If node k is labelled as "good-trustworthy" by node i, or if aF(k,j) is close to aR (i,j) then aF (k,j) is accepted by node i and is used to slightly modify the rating aR (i,j). The trust value aT (i,k) is updated leading to slightly improving the trust rate. Else the reputation rating is not modified and trust rate is decreased. The updation is based on modified Bayesian approach. The ratings are used to differentiate the nodes as misbehaving nodes or normal nodes. Hence helps in detecting malicious nodes blackhole attack and prevent them.

Updation phase (modified bayesian approach): aF(i, j) updation: Let e be the misbehaviour probability of a node j with respect to node i. The data structure F(i, j) is of the form (ra, ra) which represents the parameters of Beta distribution assumed by node i in its Bayesian view of node's j's behaviour. This prior distribution is updated as the new information becomes available. Initially the prior is Beta(1,1). Let u be the weighted discount factor for past experiences and also serving as a fading mechanism. If m is the number of observations made then u is computed as:

$$u = 1 - 1/m$$

When the new information is available, say $s^{a} \{0, 1\}$ observed deviation test for misbehaviours and f = (1-s) is the observed deviation test for normal behaviours, then the prior is updated as follows:

$$r\alpha' := ur\alpha' + s$$

$$r\alpha' := ur\alpha' + (1-s)$$

The distribution is set to $r\alpha := ur\alpha$ and $r\alpha := ur\alpha$ during the inactivity time.

T(i, j) rating: Let Φ be the probability that node j gives false information to node i, hence it uses for Φ the prior Beta(rã, rä) which is initially (1,1). This prior distribution is updated as the new information becomes available to node i from node k. Let SE {0, 1}deviation test for misbehaviours. Let v be the weighted discount factor for past experiences and also serving as a fading mechanism. If m is the number of observations made then v is computed as:

$$v = 1 - 1/m$$

The prior is updated as follows:

$$r\gamma := vr\gamma + s$$
$$r\gamma := vr\gamma + (1 - s)$$

and the deviation test is never missed. If the node k is observed as trustworthy by node i then deviation test is used to update aT (i,k) only. Else if node k is not considered as trustworthy by node i then deviation test is used to update aT (i,k) and decide whether to update aR (i,j).

R(i, j) updation: the aR (i, j) is also of the form (rα', rα'), initially set to (1,1). Direct approach: In the direct approach the prior is updated as follows:

$$r\alpha: = ur\alpha+s$$

$$r\beta = ur\beta +(1-s)$$

The distribution is set to rα = urα and rβ = urβ during the inactivity time.

Indirect approach: Trustworthiness of a node is extracted to detect and avoid fake reports. If aT (i, k) is such that node i considers node k as trustworthy, then aF (k, j) is considered by node i and the aR (i, j) is updated as follows:

$$aR (i,j) = aR(i, j)+aF(k, j)$$

which is performed for all j values contained in the report. If k is considered as untrustworthy, for each node j in the report is updated as follows: Let E (Beta(rα, rβ)) be the expectation of distribution Beta (rα, rβ):

$$aF(k, j) = (r\alpha f, r\beta f)$$

$$aR (i, j) = (r\alpha, r\beta)$$

Then, the deviation test is |E (Beta(ráf, râf)) - E(Beta(rα, rβ))| ≥d where is the deviation threshold. If the deviation test d.v≥o. Then aF (k, j) is considered incompatible and is discarded. D.V≥ O then.

Decision making phase: Based on the calulated aR (i, j) and aT(i, j) values from the previous phase node i makes the decision.

$$E (Beta (r\alpha, r\beta) <r \text{ then normal behaviour}$$

$$E (Beta (r\alpha', r\beta') \geq r \text{ then misbehaviour}$$

$$E (Beta(r\gamma, r\delta)) < t \text{ then trustworthy}$$

$$E (Beta(r\gamma, r\delta)) \geq t \text{ then untrustworthy}$$

The threshold r value is set to 0.25, if node i tolerates node j that misbehaves not more than quarter of the time. The threshold t value is set to 0.75 if i trust a node if its ratings deviate no >in 25% of the cases.

Blackhole identification phase: This phase follows many process like route discovery, route validation, data forwarding, blackhole detection etc. The routing protocol used here is AODV. The nodes follows a route discovery process to create a route between the source and the destination by broadcasting RREQ repeat request packets. As soon as the destination node/node k finds this packet, it uncast the RREP packet back to the sender with updated sequence number. This node's malicious activity or its reputation is checked in the reputation table. If the node k is found to be trustworthy, the sender sends data packets and then receiver forward ACK packet to the sender. If the node k is identified as untrustworthy then the sender doesnot send anymore packets to the node k. Reputation updation phase is executed. Node k is listed in the blacklist, hence detecting the blackhole and further preventing the routing of packets towards that particular node.

RESULTS AND DISCUSSION

Performance analysis: The proposed blackhole detection reputation based framework can be implemented using improved AODV routing protocol and simulated using NS3 in highly mobile and disconnected topologies. Performance can be computed based on number of:

- Packets sent
- Packets received
- Delay

The performance analysis and comparison in this study is based on throughput.

Throughput: Defined as "the amount of data transferred successfully on the network link over a period of time" is called throughput. It is calculated in byte sec^{-1}.

$$\text{Throughput} = (\text{No. Of bytes received})/(\text{Simulation time}) \quad \text{bytes sec}^{-1}$$

Throughput is dependent on various other metric like packet delivery fraction, path lengths, delay etc. Throughput analyzes the protocol performance, i.e., higher the throughput, better is the protocol performance (Table 1).

Table 1: Simulation parameters

Entity	Name
Tool	NS3
Protocol	AOD V/blackhole_AODV/reputation_blackhole_AODV
Simulation time	20'sec-100'sec
Perormance parameter	PDR Throughtput end to end delay
Mobility model	Randorn waypoint mobility model
Date rate	64 byte sec^{-1}
Traffic	CBR
Data packer size	64 bytes
Number of mobile nodes	20-100
Speed	20 m^{-1}
Transmission area	300×1500 m

The simulation results are plotted into graphs with x-axis as the time vs y-axis as the throughput. Throughput analysis of blackhole aodv, the througput analysis of reputation based blackhole AODV and the comparison of throughput analysis in all the three cases.

CONCLUSION

In this study, we have proposed framework for detecting blackhole attacks in MANETS using direct and indirect aproach. The proposed framework's architecture, data structures used and its phases, implementation and simulation details with the performance analysis are discussed in the study. The performance efficiency of the proposed framework can be analyzed in the presence and absence of blackhole nodes in the network using the plain AODV and improved AODV as the routing protocol. From the simulation it is observed reputation based model with direct and indirect reputation computations performs better when there is a blackhole existing in the network. The number of packets dropped are fairly reduced and packets are rerouted based on the reputation calculations.

REFERENCES

Bansal, S. and M. Baker, 2003. Observation-based cooperation enforcement in ad hoc networks. Technical Report, July 6, 2003, Stanford University, Stanford, CA., USA., pp: 1-10. http://arxiv.org/pdf/cs.ni/0307012.pdf.

Buchegger, S. and J.Y. Le Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 9-11, 2002, Lausanne, Switzerland, pp: 226-236.

Buchegger, S., J. Mundinger and J.Y.L. Boudec, 2008. Reputation systems for self-organized networks. IEEE. Technol. Soc. Mag., 27: 41-47.

Cho, J.H., A. Swami and I.R. Chen, 2010. A survey on trust management for mobile ad hoc networks. IEEE Commun. Surv. Tutorials, 13: 562-583.

Mahmoud, A., A. Sameh and S. El-Kassas, 2005. Reputed authenticated routing for ad hoc networks protocol (reputed-ARAN). Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems, November 7-7, 2005, IEEE, Cairo, Egypt, ISBN:0-7803-9465-8, pp: 8-8.