IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 5, May 2014, 43-50

REVIEW ON REPUTATION SCHEMES OF DSR IN MOBILE AD HOC NETWORK

SANTOSH KUMAR[1] & SUVEG MOUDGIL[2]

[1]Research Scholar, Haryana Engineering College, Jagadhri, Haryana, India

[2]Associate Professor, Haryana Engineering College, Jagadhri, Haryana, India

ABSTRACT

Mobile ad-hoc networks are prone to a number of security threats. Handling misbehaviour Nodes is a difficult issues in ad hoc network so trust schemes is an important issue to be considered in network for efficient routing. Reputation of a node can be calculated using a simple formula and a node is supposed to maintain a good reputation value to participate in route discovery process. The main objective of this research paper is to survey various reputation schemes where nodes monitor their neighbourhood & detects several kinds of misbehaviour such as partial packet dropping, receiver collisions and transmission power.

KEYWORDS: Mobile Ad Hoc Network, Reputation Schemes, Routing, DSR

INTRODUCTION

Mobile Ad hoc Network is a collection of free mobile nodes that can converse to each other through radio waves. The mobile nodes that are in radio range of each other can directly communication, whereas others need the aid of in-between nodes to route their packets. These networks are fully scattered, and can work at any place with no the help of any communications. This property makes these networks extremely exible and robust. There are few characteristics of these networks are communication through wireless communication and nodes can perform the roles of both hosts and routers [1]. There are no centralized controller and infrastructure in mobile ad hoc network and natural mutual trust in between the nodes.

ROUTING PROTOCOLS

In Mobile ad hoc network the routing is a difficult task and it is very different from routing protocols in traditional wired world. [20] some of reasons are mobile ad hoc network are frequently route updates topology changes due to failures of nodes. There are limited transmission ranges of nodes in mobile ad hoc network.

PROACTIVE PROTOCOLS

Proactive routing protocols maintain routes to all destinations, apart from of whether or not these routes are needed. In order to maintain exact route information, a node must from time to time send manage messages. So, proactive routing protocols may waste bandwidth since organize the messages are sent out without need when there is no data traffic. [20] The main benefit of this type of protocols is that hosts can quickly obtain route information and quickly establish a session. For example, Global State Routing is based on the Link State routing method. In the LS routing method, each node floods the link state information into the whole network once it realises that links change between itself and its neighbours. The link state information includes the delay to each of its neighbours. A node will know the whole topology when it obtains all link information.

REACTIVE PROTOCOLS

Reactive routing protocols can considerably reduce routing transparency because they do not need to search for and maintain the routes on which there is no data traffic [20]. This property is very attractive in the resource-limited environment.

DYNAMIC SOURCE ROUTING

Dynamic Source Routing uses source routing to deliver packets from one node in the network to some other node. The source node adds the full path to the destination in terms of intermediate nodes in every packet [1, 6 and 9]. This information is used by intermediate node to determine whether to accept the packet and to whom to forward it. DSR operates on two mechanisms are followings

- Route Discovery
- Route Maintenance

Route discovery is used when the sender does not know the path up to the destination. In this mechanism, the sender broadcasts a route request message which contains source address, destination address, and identifier. Each intermediate node adds its address in route request message and rebroadcast it, unless it has not rebroadcast earlier. With this controlled broadcast, the route request will ultimately reach the destination. The destination then sends a unicast route reply message in reverse direction whose information is obtained from list of intermediate nodes in route request message. When the route reply packet reaches the source, it records the route contained in it and saves in its cache for the specific destination. For better performance, intermediate nodes also record this route information from the two route messages. All nodes overhearing these packets add meaningful route entries in their caches. Finally, route maintenance mechanism is used to notify source and potentially trigger new route discovery events when changes in the network topology invalidates a cached route [5].

REPUTATION SCHEMES

- In the confident scheme of reputation, a routing protocol for mobile ad hoc network based on Dynamic Source Routing protocol. Upon finding of the nodes spite, its packets are not forward by normally behaving of nodes, while it is avoided in case of a routing decision & deleted from a path cache. The structural design comprises four mechanisms residing on each node first are the Monitor, second is the Reputation System third is the Path Manager and forth is the faith Manager components. The monitor components enable nodes to identify deviation on the next node on the source route by either listening the transmission of the observing rout protocol behavior, an alarm message is sent to the faith manager component, where the source of the message is evaluate. The evaluation is updated only if there is satisfactory evidence of malicious behaviour that is significant for a node and that has occurred a number of times, more than a threshold to rule out of coincidence for example is collision Evidence could come either from a node's own experiences through the Monitor system or from the faith Manager in the form of Alarm messages and second-hand information is attributed with low worth with respect to the first-hand information, irrespective of its source node. Black lists may be used in a route request so as to avoid bad nodes along the way to the destination or to not handle a request originating from a malicious node and in forward packet requests, so as to avoid forward packets for nodes [13].

- In the Collaborative Reputation scheme differentiate the selfish node and malicious node of reputation on the Dynamic Source Routing protocol. It stimulates node relationship through monitoring of the cooperativeness of nodes and a reputation method. It uses first and second-hand experience, combined by a specific function. This function is used by the Watchdog mechanism for the evaluation of other nodes' performance. If the observed behavior is different than the outcome of this function then the rating of the observed node is changed. Each node of the network monitors the behavior of its neighbors, with respect to the requested function, and collects remarks about the implementation of that function. These observations are recorded to the reputation table maintained by each node. Each row of the table corresponds to a neighbor node and consists of four entries, regarding the monitored function: the unique id of the node, a collection of firsthand observations made on the node's behavior [16].

The nodes which not help with other nodes in the le ad hoc network, for saving battery for its own communication is called selfish node while these nodes does not damage other node. The malicious node in mobile ad hoc network behaves abnormally and can damage other nodes by doing any doubtful activity. This scheme purposed three different type of reputation: first is Subjective Reputation: - Reputation value evaluated by giving priority to past observation of mobile node than current one. If malicious node is found out then node's subjective reputation value is changed by using watchdog mechanism. Second is Indirect Reputation: -- This value is calculated by providing reputation by one node to other node. Reputation value can be updated through reply message that contains the list of nodes behave normally in situation of each function. If any node having negative reputation value all requested by that node will be rejected and this node works only as service provider not as requester. For long period of time if this node will provide correct services to all other nodes in mobile ad hoc network, node can achieved their reputation value again. When reputation value is more than the threshold reputation value, that node will again works as service source as well as service requester. Third is functional Reputation: - This reputation is the combination of indirect and subjective reputation value. To calculate the functional reputation value using weights combine formula.

- In the ACK mechanism, Kejun et al. focused on to finding the misbehaving links instead of misbehaving nodes and which may be used as an attach to the existing source routing protocols, such as Dynamic source routing. The scheme makes use of a special acknowledgment packet which has been assigned a fixed route of three nodes in the opposite direction of the actual data traffic flow. Three nodes n1, n2, and n3 are assumed to lie along the path from source to destination. When n1 node forwards a packet to n3 node through n2 node, n1 node will not be sure whether n3 received the packet due to the misbehaviour or ambiguous collisions in the path. In order to confirm the packet reception n3 will send an ACK packet to n1 via n2, called 2ACK. Among the triplet, n1 is the observer of the link n2 to n3. This formation is carried out along the whole path. For every outgoing packet n1 will store the ID of the packet for time t in a list it maintains. When an ACK is received for a packet and matched to an id in the list before time t expires, the entry in the list is discarded and a special counter is incremented and Counter miss is incremented otherwise. After a time period the ratio of missed counter and counter packet is compared with a preset threshold, if the ratio is greater than the threshold all nodes are reported regarding the misbehaving link n2 to n3 by sending a RERR message. Each node receive a request route message deems n2 to n3 as a misbehaving link. These links are then avoided in the future. Nodes such as n2 should not change the 2ACK packet passing through them; a one way hash chain mechanism [17]

PASSIVE ACKNOWLEDGEMENTS

In passive acknowledgement scheme, the nodes make use of overhear something method to listen to other nodes transmission. By overhearing neighboring nodes broadcast, a node can recognize whether its neighbor forwards its packet to other node without any disinclination.

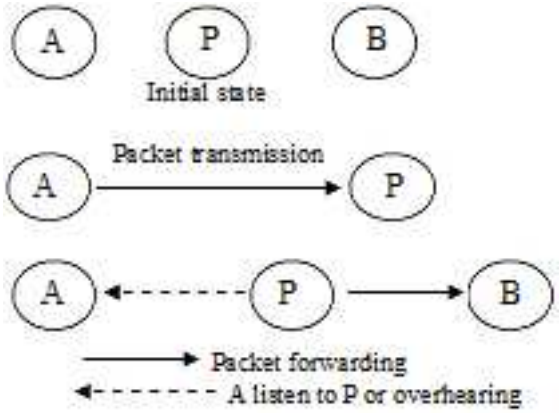

Figure 1: Passive Acknowledgements

Table 1: Comparison of Schemes

S. No	Scheme	Observation	Detection	Advantages	Limitations
1	Confidant	Passive	Single Node	Selfish nodes are separated and faith recommendation is use into account.	Observation is based on passive acknowledgement.
2	CORE	Passive	Single Node	Second chance is given for nodes in bad locations and no negative ratings are communicated.	Dependence on passive acknowledgement, more weight is given to previous behaviour and therefore recent Misbehavior will be observed.
3	2ACK	Active	Single Node	Use active acknowledgments for two hop to mixture the problems in loose listening.	What happens when a 2Ack got lost or dropped by a malicious node

Problems in Passive Acknowledgement

Most of the reputation based schemes make use of passive acknowledgments to observe their neighbors for packet forward activities. Individually from its compensation, such as the fact that it needs no specialized hardware ensuring low cost, it has several disadvantages which are caused by the peculiarities of mobile ad hoc networks. Identify the following weaknesses of the Watchdog mechanism in the presence of which it might not detect a selfish or misbehaving node.

ACTIVE ACKNOWLEDGEMENTS

In active acknowledgment scheme requires nodes to clearly acknowledge the sender node about the successful response of packet transmission. If an unambiguous acknowledgement reaches the source node from the destination node and the source can make sure that all intermediate nodes in the transmission path are well behaved nodes & they have forward packets to the destination node.

LITERATURE REVIEW

Rajesh Sharma et al. They had discussed a solution on the basis of reputation method to solve routing issues raised by misbehaving nodes [1].

Sohail Abbas et al. The author survey and categorize reputation based schemes according to their passive and active acknowledgment monitoring techniques in multi hop networks such as mobile ad hoc networks selfish or misbehaving nodes can disrupt the whole network and severely degrade network performance[2].

Renu Dalal et al The authors provide the different ways to achieve trust in mobile Ad-hoc Network. Providing safe communication between mobile nodes, reorganization the position of nodes, reducing overhead, handling misbehaviour and location updates are such a difficult issues in ad-hoc network so providing trust schemes is an important in this network [3]

Santhosh Krishna B. Vet et al. The author focus on single and multiple black hole attacks. The implementations of black hole comprises active routing misbehaviour and forwarding misbehaviour & design and build our prototype over DSR and test it in Network simulator 2 in the presence of variable active black hole attacks in highly mobile and sparse networks [5].

Isaac Woungang et al. provide a novel scheme for Detecting Black Hole Attacks in MANETs is introduced. The BDA-DSR protocol detects and avoids the black hole problem before the actual routing mechanism is started by using fake route request packets to catch the malicious nodes [6].

Poonam K Gar et al. They had discussed and proposed a new algorithm to find route to the destination as a weighted average of the trust value of the nodes in the route, with respect to its behavior observed by its neighboring nodes and the number of nodes in the route is calculated [9].

Sangheetaa Sukumran et al. the author had proposed a new reputation based routing protocol based on DSR. This approach calculates the reputation values of the nodes using simple formula. Any node is supposed to maintain a good reputation value in order to receive network services [10].

CONCLUSIONS

Secure routing is must for ad hoc network. DSR protocols based on various reputation schemes have been studied. A secure and efficient route to the destination is calculated on the basis of reputation value of the node. Thus a node needs to maintain a good reputation value in order to enjoy network services. A misbehaving node which is isolated has no chances of rejoining the network until the entire network is reformed. A node with low reputation value is not allowed to participate in network as it will decrease the efficiency & effectiveness of the network. Passive acknowledgment techniques are more promising than active acknowledgment techniques as they do not cause any extra communication or memory overhead. Active acknowledgment provides reliability at the cost of extra memory and communication overhead but in the environments where there is a high collision rate it is as prone to errors.

REFERENCES

1. Rajesh Sharma & Seema Sabharwal “Dynamic Source Routing Protocol (DSR)”, IJARCSSE, Volume 3, Issue 7, July 2013 pp. 239-241.

2. Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones “A Survey of Reputation Based Schemes for MANET” 2010.
3. Renu Dalal1, Manju Khari and Yudhvir Singh “Different Ways to Achieve Trust in MANET” International Journal on Ad Hoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.
4. G. Rajkumar, R. Kasiram and D. Parthiban “Optimized QoS Metrics and Performance Comparison of DSR and AODV Routing Protocols”, IEEE-International Conference On Advances In Engineering, Science and Management (ICAESM -2012) March 30, 31, 2012. On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.
5. Santhosh Krishna B.V, Mrs. Vallikannu A.L “Detecting Malicious Nodes for Secure Routing in MANETS Using Reputation Based Mechanism” International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010.
6. Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi and Mohammad S. Obaidat, Fellow of IEEE and “Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks”, 2012.
7. Ramasamy Mariappan Sangameswaran Mohan “Re-pro Routing Protocol with Trust based Security for Broadcasting in Mobile Ad hoc Network” IEEE 2011.
8. Sangheethaa Sukumaran, Venkatesh. J, Arunkorath “A Survey of Methods to mitigate Selfishness in Mobile Ad hoc Networks” International Journal of Information and Communication Technology Research Volume 1 No. 2, June 2011.
9. Poonam, K. Garg, M. Misra “Trust Based Multi Path DSR Protocol”, International Conference on Availability, Reliability and Security IEEE 2010.
10. Sangheetaa Sukumran, Venkatesh Jaganathan, Arun Korath “Reputation based Dynamic Source Routing Protocol for MANET” International Journal of Computer Applications (0975 – 888) Volume 47– No.4, June 2012.
11. E. Friedman, P. Resnick, and R. Sami, "Ch: 27- Manipulation-Resistant Reputation Systems," in Algorithmic Game Theory, N. Nisan, V. V. Vazirani, E. Tardos, and T. Rough garden, Eds. New York: Cambridge University Press, 2007, pp. 677-697.
12. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks" in Proceedings of the 6th annual international conference on Mobile computing and networking Boston, Massachusetts, United States: ACM, 2000.
13. S. Buchegger, J. Yves, and L. Boudec, "Performance analysis of the CONFIDANT protocol" in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing Lausanne, Switzerland: ACM/IEEE, 2002.
14. S. Buchegger, L. Boudec, and Jean-Yves, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks," in Proceedings of Wi Opt `03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, France, 2003.

15. Sonja and Buchegger, "A robust reputation system for P2P and mobile ad-hoc networks," in Proceedings of P2PEcon, Harvard University, USA, 2004.
16. P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Kluwer, B.V., 2002.
17. L. Kejun, D. Jing, K. V. Pramod, and B. Kashyap, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE Transactions on Mobile Computing, vol. 6, pp. 488-502, 2007.
18. L. Zhao and J. G. Delgado-Frias, "MARS: Misbehavior Detection in Ad Hoc Networks" in IEEE Global Telecommunications Conference (GLOBECOM) 2007, pp. 941-945.
19. K. Graffi, P. S. Mogre, M. Hollick, and R. Steinmetz, "Detection of Colluding Misbehaving Nodes in Mobile Ad Hoc and Wireless Mesh Networks" in IEEE Global Telecommunications Conference (GLOBECOM) 2007, pp. 5097-5101.
20. Anu Saxena*1, Ved Prakash2, simulation study of AODV and DSR routing protocol in wireless ad-hoc networks IJESR/Aug 2012/ Volume-2/Issue-8/Article No-3/741-748.