IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

A Collaborative Contact-Based Watchdog CoCoWa for Detecting Selfish Nodes with Trust Model

P. Anitha[1], Dr.G.Satyavathy[2]

Department of Computer Science, Bharathiar University, India[1,2]

Abstract: Mobile ad-hoc networks (MANETs) assume that mobile nodes volunteer collaborates in order to work appropriately. This Cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to selfish node behaviour. Thus, the complete network performance could be seriously affected. The use of watchdogs is a well-known mechanism to detect selfish nodes. However, the detection process performed by watchdogs can fail, generating false positives and false negatives that can induce to wrong operations. Moreover, relying on local watchdogs alone can lead to poor performance when detecting selfish nodes, in term of precision and speed. This is especially important on networks with sporadic contacts, such as Delay Tolerant Networks (DTNs), where sometimes watchdog's lack of enough time or information to detect the selfish nodes. Thus, Collaborative Contact-based Watchdog (CoCoWa) is proposed as a collaborative approach based on the diffusion of local selfish nodes awareness when a contact occurs, so that information about selfish nodes is quickly propagated. As shown in the paper, this collaborative approach will make the selfish node as trusted node by using AODV protocol and provide better security.

Keywords: CoCoWa Architecture, Watchdog, Delay Tolerant Networks, Trust model, Security, Routing Protocol, and AODV.

I. INTRODUCTION

1.1 OVERVIEW OF THE MANET

Recent advancements in wireless communication and the miniaturization of computers have led to a new concept called the mobile ad hoc network (MANET), where two or more mobile nodes can form a temporary network without need of any existing network infrastructure or centralized administration.[1] Even if the source and the destination mobile hosts are not in the communication range of each other, data packets are forwarded to the destination mobile host by relaying transmission through other mobile hosts which exist between the two mobile hosts. Figure.1.1 shows that how the messages are sending from source to destination in MANET. Since no special infrastructure is required, in various fields such as military and rescue affairs, many applications are expected to be developed for ad hoc networks.

In ad hoc networks, since mobile hosts move freely, disconnections occur frequently, and this causes frequent network partition. If a network is partitioned into two networks due to the migrations of mobile hosts, mobile hosts in one of the partitions cannot access data items held by mobile hosts in the other. Thus, data accessibility in ad hoc networks is lower than that in conventional fixed networks. In ad hoc networks, it is very important to prevent the deterioration of data accessibility at the point of network partition. A possible and promising solution is the replication of data items at mobile hosts which are not the owners of the original data.

Since mobile hosts generally have poor resources, it is usually impossible for them to have replicas of all data items in the network.

For example, let us suppose a situation where a research project team engaged in excavation work constructs an ad hoc network on a mountain. The results obtained from the investigation may consist of various types of data such as numerical data, photographs, sounds, and videos. In this case, although it is useful to have the data that other members obtained, it seems difficult for a mobile host to have replicas of all the data.

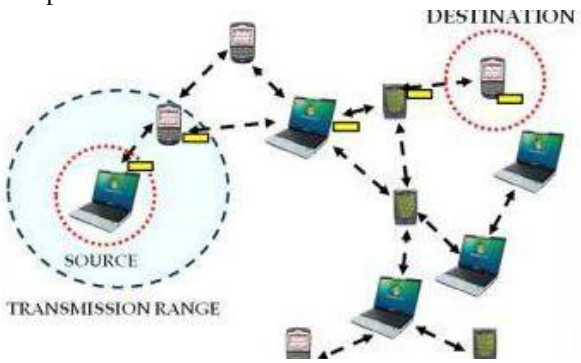

Figure 1.1: MANET

II. COCOWA

Mobile ad-hoc networks (MANETs) assume that mobile nodes controlled collaborate in order to work properly. CoCoWa (Collaborative Contact based Watchdog) is a new scheme for detecting selfish nodes that combines local watchdog detections and is used in the dissemination of information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs. In this method, nodes have second hand information about the selfish nodes in

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

the network. The goal of this approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives.

A selfish node usually denies packet forwarding in order to save its own resources. This Behaviour implies that a selfish node neither participates in routing nor relays data packets. [5]A common technique to detect this selfish Behaviour is network monitoring using local watchdogs. A node's watchdog consists on overhearing the packets transmitted and received by its neighbours in order to detect anomalies, such as the ratio between packets received to packets being re-transmitted. [4]By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfishly (or not) It is based on the combination of a local watchdog and the diffusion of information when contact occurs between pairs of nodes. [34]A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them).

Assuming that there is only one selfish node, the figure 2.1 shows how initially no node has information about the selfish node. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non-selfish node, it is marked as a negative. Later on, when this node contacts [2]another node, it can transmit this information to it; so, from that moment on, both nodes store information about this positive (or negative) detections.

The Diffusion module has two functions: the transmission as well as the reception of positive (and negative) detections. [6]A key issue of this method is the diffusion of information. As the number of selfish nodes is low compared to the total number of nodes, positive detections can always be transmitted with a low overhead. Transmitting only positive detections has a serious drawback: false positives can be spread over the network very fast. [7]Thus, the transmission of negative detections is necessary to neutralize the effect of these false positives, but sending all known negative detections can be troublesome, producing excessive messaging or the fast diffusion of false negatives.

Consequently a negative diffusion factor γ that is the ratio of negative detections that are actually transmitted. This value ranges from 0 (no negative detections are transmitted) to 1 (all negative detections are transmitted). A low value for the γ factor is enough to neutralize the effect of false positives and false negatives. Finally, when the diffusion module receives a new contact event from the watchdog, it transmits a message including this information to the new neighbour node.[11][12]When the neighbour node receives a message, it generates an event to the network information module with the list of these positive (and negative) detections.

Behaviour of malicious nodes is modeled from the receiver perspective, which is based on the probability of receiving wrong information about a given node. When that given contact node occurs with a malicious node that is, it receives a Negative about the selfish node, and a Positive about the other nodes. Thus the above Behaviour as the maliciousness probability. Several aspects that can affect this probability is given below.

1) The reception of information, considering that not all contacts produce this reception. This aspect is similar to the collaboration degree (that is, the pc parameter), but an increase of communication range of the malicious nodes will increase the information reception.

2) The malicious nodes do not have information about all nodes; so, in order to send a positive/negative about a node, they must have contacted this node previously or have received a message from other nodes.

3) Another issue to consider is the proper generation of wrong information, for example when receiving a positive of a node that is not a selfish node. [35]From the receiver point of view, a perfect malicious node will always provide wrong information. In this case, the malicious node, in order to send wrong information, must know the state of each node. In other words it must have a perfect local watchdog (about the node it contacts).

4) MAC layer selfish misbehavior in IEEE 802.11 ad hoc networks. In such networks selfish nodes can manipulate the following MAC layer parameters to enhance their channel access probability:

Duration of the rest of the transmission (or the remaining transmission duration), SIFS (Secret Internet Fatties) duration, DIFS (Distributed Inter-Frame Space) duration, and back off time.

Specifically, when sending RTS or DATA frames, by increasing the included duration value, a selfish node can claim to occupy the channel for a longer period to prevent other normal nodes from contending for the channel.

[10]A selfish node may also choose a smaller SIFS duration so as to finish its current transmission quickly to initiate the next one. [11]In addition, by setting DIFS to a smaller value after sensing the channel idle, a selfish node will wait for a shorter time interval to start the back off process and may have higher channel access probability

- Naive strategy: A selfish node always chooses a small constant value as its back off time.[18]
- Random strategy: Instead of choosing a small constant back off time, a selfish node randomly chooses its back off time from a smaller fixed contention window than that of normal nodes, for example, 1⁄20; CWmin =4Š . [17]Thus, the selfish nodes expected back off period is smaller than that of normal nodes.
- G-Persistent strategy: Instead of choosing a fixed contention window size, a selfish node still follows the IEEE BEB (Binary Exponential Back off) rule to double its contention window size in case of retransmissions. [16] However, its back off time is determined by multiplying a randomly chosen value in current contention window by a control parameter in current contention window.

DOI 10.17148/IJARCCE.2016.5296

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

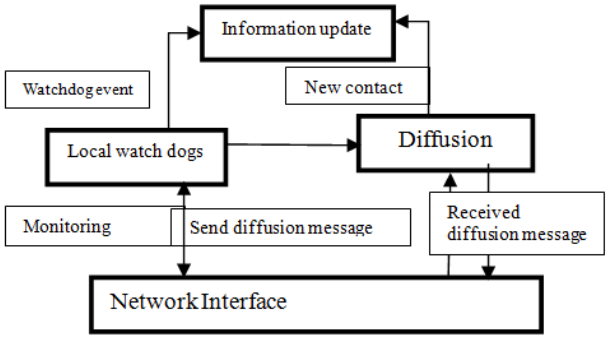

Figure 2.1: CoCoWa Architecture

The major characteristics of selfish nodes include the following:

- Do not participate in routing process
- Do not reply or send hello messages
- Intentionally delay the RREQ packet
- Dropping of data packet

Disadvantages of COCOWA

- The selfish nodes was Increased
- The packet loss was Increased
- Throughput was reduced
- Overhead was Increased
- Selfish nodes can seriously degrade the performance of packet transmission.

III. TRUST MODEL

3.1 AODV Protocol:

AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. [31]This algorithm was motivated by the limited bandwidth that is available in the media that are used for wireless communications. [32] It borrows most of the advantageous concepts from DSR and DSDV algorithms. The on demand route discovery and route maintenance from DSR and hop-by-hop routing, usage of node sequence numbers from DSDV make the algorithm cope up with topology and routing information.[22] Obtaining the routes purely on-demand makes AODV a very useful and desired algorithm for MANETs.

3.2TRUST BASED COCOWA ROUTING PROTOCOL

COCOWA along trust model is incorporated with AODV routing protocol in order to prevent the malicious behavior and to achieve uniform utilization of network resources.
The AODV protocol is modified as described below.

1. AODV sends RREP (Route REPly)packet for each RREQ (Route REQust packet it receives, thereby enabling AODV to make the destination sends multiple RREP packets for single route request reception of information, considering that not all contacts produce this reception.[19] This aspect is similar to the collaboration degree.

2. RREP involves sending the acknowledgement message from destination to the source. After receiving this message from RREP, the source sends the actual message to destination[20]

3. The routing table structure is modified to store the trust value for each entry of source to destination when receiving a positive value of a node that is not a selfish node.[21] From the receiver point of view a perfect malicious node will always provide wrong information. In this case, the malicious node, in order to send wrong information must know the state of each node.

4. AODV sends request to update the routing path at regular intervals. Hence, at regular intervals, source node is going to have multiple paths. Each paths having its trust value from which one with the maximum trust is selected.[24] It can transmit this information to it so, from that moment on, both nodes store information about this positive (or negative) detections. [21][23]Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative transmission of information that is provided by other nodes

5. A node detecting a selfish node using its watchdog is marked as positive, and if it is detected as a non-selfish node, it is marked as negative. [26]The method to handle RREP packet is changed to update the route entry when new path is received with greater trust than current trust value to send RREQ packet to destination every time thereby disabling the mechanism to initiate RREP packet at intermediate nodes[27][28].

Type	R A D G	Reserved	Hop count
RREQ ID			
Postive(local) Postive(Indirect) Negative(local) Negative(indirect)			
RREQTime RREQRecvStrength RREQ Info			
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Originator Sequence Number			
Lifetime			
Trust of path			

Table 3.1: Packet format

Table 3.1 shows about packet format for the trusted model and the type of node and fields of RADG. RREQID is route request ID to calculate message for sending actual message. Reply for the messages are sent after calculating positive or negative event for the node messages. The time should be limited for trusting the node with strength. The IP address and sequence number is to transmit the message from source to destination. Life time is calculated based on how long the message is sent to the destination in trust path.

3.3 ADVANTAGES OF PROPOSED SYSTEM

- Reduction of selfish nodes
- Increase in throughput

4. STEP BY STEP REPRESENTATION FOR DETECTING SELFISH NODE

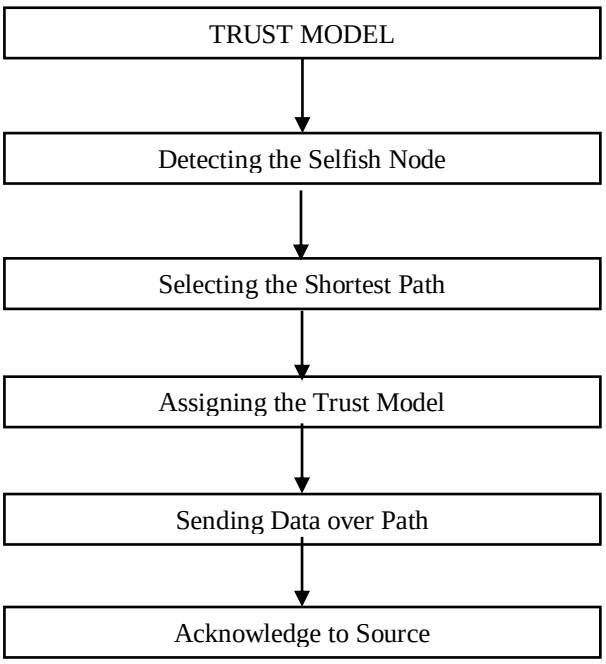

Figure 4.1 Step by step selfish Node Detection

IV. SIMULATION TOOLS

NS-2 is used to simulate the ANFIS algorithm. In our simulation, the channel capacity of mobile hosts is set to the 2 Mbps. For the MAC layer protocol the distributed coordination function (DCF) of IEEE 802.11 (for wireless LANs) is used. It has the functionality to notify the network layer about link breakage. In the simulation, mobile nodes move in a 500meter x 500 meter region for 50 seconds simulation time.[29][30] The number of mobile nodes is varied from20 to 100. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250meters. In our simulation, the speed is set as 2m/s. The simulated traffic is Constant Bit Rate (CBR).The pause time of the mobile node is kept as 10sec.

V. CONCLUSION

CoCoWa can reduce the effect of malicious or collusive nodes. If malicious nodes spread false negatives or false positives in the network CoCoWa is able to reduce the effect of these malicious nodes quickly and effectively. Additionally CoCoWa is also effective in opportunistic networks and DTNs, CoCoWa can reduce the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced overhead (message cost). This reduction is very significant, ranging from 20% for very low degree of collaboration to 99% for higher degrees of collaboration.

VI. FUTURE WORK

In future,there is a possibility of different types of attacks that exploit the routing algorithm itself. Cooperative bait detection scheme (CBDS) is presented that effectively detects the malicious nodes that attempt to launch gray hole/collaborative blackhole attacks. In this scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list.

REFERENCES

[1] What is MANET and its protocols http://manetattacks.blogspot.in/2012/10/what-ismanet.html .HarjeetKaur et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 498-500 www.ijcsit.com 500

[2] C.Siva Ram Murthy and B.S.Manoj. Ad Hoc Wireless Networks Architectures and Protocols. PRENTICE HALL, 2004.

[3]. Priyanka Goyal, Vinti Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[4]. Gagandeep, Aashima and Pawan Kumar "Analysis of Different Security Attacks in MANETs on Protocol Stack". International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012

[5]. Mohammad Wazid , Rajesh Kumar Singh and R. H. Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques " International Journal of Computer Applications® (IJCA) International Conference on Computer Communication and Networks CSI-COMNET- 2011.

[6]. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao " A survey of black hole attacks in wireless mobile ad hoc networks" Human-centric Computing and Information Sciences 2011

[7] Sunil Taneja and Ashwani Kush, " A Survey of Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, 279-285, August 2010.

[8] Gary Breed Editorial Director, "Wireless Ad-Hoc Networks: Basic Concepts", High Frequency Electronics, March 2007.

[9] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks" IEEE Communications Magazine • October 2002

[10] Mohseni, S.; Hassan, R.; Patel, A.; Razali, R, "Comparative review study of reactive and proactive routing protocols in MANETs", 4th IEEE International Conference on Digital Ecosystems and Technologies, 304-309, 2010.

[11] Humayun Bakht, " Survey of Routing Protocols for Mobile Ad-hoc Network", International Journal of Information and Communication Technology Research, 258-270, October 2011.

[12] Mohit Kumar and Rashmi Mishra "An Overview of MANET: History, Challenges and Applications" , Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[13] C. Perkins, E. Belding-Royer and S. Das, "Ad-Hoc On-Demand Distance Vector (AODV) Routing", RFC3561, July 003

[14] Xu Huang, Muhammad Ahmed and Dharmendra Sharma"Protecting from Inside Attacks in Wireless Sensor Networks" 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[15] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao "A survey of black hole attacks in wireless mobile ad hoc networks" Tseng et al. Humancentric Computing and Information Sciences 2011, a Springer open journal.

[16] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala "DoS Attacks in Mobile Ad-hoc Networks: A Survey" 2012 Second International Conference on Advanced Computing & Communication Technologies.

[17] Harmandeep Singh, Gurpreet singh and Manpreet Singh "Performance Evaluation of Mobile Ad Hoc Network Routing Protocols under Black Hole Attack"International Journal of Computer Applications (0975 – 8887) Volume 42– No.18, March 2012.

[18] HimaniYadav and Rakesh Kumar "Identification and Removal of Black Hole Attack for Secure Communication in MANETs" Volume 3, Issue 9, September 2012, ISSN 2047-3338.
[19] Morigere Subramanya Bhat, Shwetha .D, Manjunath .D and DevarajuJ.T."Scenario Based Study of on denmand Reactive Routing Protocol for IEEE-802.11 and 802.15.4 Standards" ISSN: 2249-57 Vol 1(2), 128-135 published in October-november 2011.
[20] Ning.P. and Sun.K. How to misuse aodv: a case study of insider attacks against mobile ad-hoc routing protocols. Technical report, Comput. Sci. Dept., North Carolina State Univ., Raleigh, NC, USA, 2003.
[21] Ashish Bagwari,Raman Jee,Pankaj Joshi,Sourabh Bisht "Performance of AODV Routing Protocol with increasing the MANET Nodes and it's effects on QoS of Mobile Ad hoc Networks" 2012 International Conference on Communication Systems and Network Technologies.
[22] Naveen Bilandi and Harsh K Verma "Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET" International Journal of Electronics and Computer Science Engineering 1660 ISSN- 2277-1956.
[23] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad Comparison of AODV and DSR on-Demand Routing Protocols in Mobile Ad hoc Networks.
[24] Prem Chand and M.K. Soni "Performance comparison of AODV and DSR ON-Demand Routing protocols for Mobile ad-hoc networks" Published in July 2012.
[25] Michel Healy, Thomas News and Elfed Lewis "Security for Wireless Sensors Networks: A Review".in Feb 2009.
[26] David B. Johnson Josh Broch, David A. Maltz and Jorjeta Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. Technical report, Computer Science Department, Carnegie Mellon University, Pittsburgh, PA 15213, USA.
[27] IrshadUllahShoia Ur Rehman "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols".
[28] ShailyMittel and PrabhjotKaur "Performance comparison of AODV, DSR and ZRP Routing protocol in MANET's" Published in 2009.
[29] NicklesBeijar "Zone Routing Protocol" Networking Laboratory, Helsinki University of Technology.
[30] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.
[31] JosephinJeneba Y, Prabakaran T, "Detection of Selfish Node in Manet using a Collaborative Watchdog", international journal of engineering sciences & research Technology, ISSN: 2277-9655, May 2013
[32] Jae Ho Choi, Kyu Sun Shim, Sang Keun Lee, and Kun Lung Wu, "Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network", IEEE Transactions on mobile computing, Vol 11, no. 2,pp.278-291,February 2012
[33] Enrique Hern andez -Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog", IEEE Communications letters, Vol. 16, no. 5, May 2012
[34] L Yin and G Cao, "Balancing the Tradeoffs between Data Accessibility and Query Delay in Ad Hoc Networks", Proc. IEEE Int'l Symp. Reliable Distributed Systems, pp. 289-298, 2004
[35]K Balakrishnan, J Deng, and P K Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless Comm. And Networking, pp. 2137- 2142, 2005

DOI 10.17148/IJARCCE.2016.5296