IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Volume-03, Issue-09 E-ISSN: 2347-2693

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

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

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

www.ijcseonline.org

Received: Sep /03/2015 Revised: Sep/10/2015 Accepted: Sep/24/2015 Published: Sep/30/ 2015

***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, AODV

I. INTRODUCTION

A MANET is a type of ad- hoc network that can change positions and construct itself on the fly. MANET can be a model of Wi-Fi connection, or another standard, like a cellular or satellite transmission. MANET has many applications like military, communication, conference meeting, automated battlefield, creating virtual classrooms and in sensor networks. The key features of MANET are restoring and self-organizing and transmission is done through multiple hops Topology because nodes are self-managed without any preexisting structure. MANET has different characteristics like bandwidth constraint and limited physical security. MANET used routing protocols for sending data from source to destination [1] [2] [3]. Mobile ad hoc networks are a collection of mobile nodes, which configures itself. The nodes itself act as a transmitter and receiver in the case of node communicating within the radio range [5] [6].If two nodes are not within the transistor range, announcement takes place by spreading packets with the teamwork of other nodes in the network. The open medium and remote circulation of MANET makes it vulnerable to various types of attacks. Therefore an interference recognition system must be used to advance the security in MANET. Watchdog scheme [7] [8] [9] [10] listens to its next hop transmission. If the node fails to onward the packet to the next hop, the watchdog rises the security value. If the counter value outdoes the threshold value, it reports the node as malicious. Path rater [8] works in collaboration with the routing protocols in path collection. In TWO ACK scheme, the mischievous links can be distinguished. In this scheme, acknowledgement packets are transmitted for three successive nodes from source to terminus. But the acknowledgement packet produces the network overhead which radically reduces the network presentation and consumes more battery-operated power. We detailed our COCOWA along trust model with AODV routing protocol in order to prevent the malicious node behavior and uniform utilization of network resources.

II. OVERVIEW OF COCOWA ARCHITECTURE

A selfish node usually repudiates packet forwarding in order to save its own resources. This behaviour implies that a selfish node neither contributes in routing nor relays data packets [10]. A common method to detect this selfish performance is network nursing using local watchdogs. A node's watchdog contains on eavesdropping the packets conveyed and straight reports the irregularities, such as the ratio between packs received to packs being retransmitted [11]. By using this technique, the local watchdog can produce a positive (or negative) detection in case the node is acting selfishly (or not). An example of how CoCoWa works is outlined in Fig. 1. It is based on the combination of a local watchdog and the dispersal of information when a contact between pairs of nodes occurs. A contact is defined as an opportunity of broadcast 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 shows how originally no node has data about the selfish node. When a node detects a selfish node using its watchdog, it is obvious as a positive, and if it is perceived as a non-selfish node, it is marked as a negative. Later on, when this node links another node, it can transmit this data

to it; so, from that moment on, organized nodes store information about these positive (or negative) detections. Therefore, a node can develop conscious about selfish nodes straight (using its watchdog) or circuitously, through the collaborative transmission of information that is provided by other nodes. Under this scheme, the unrestrained diffusion of positive and negative detections can produce the fast diffusion of incorrect information, and therefore, a poor network performance.

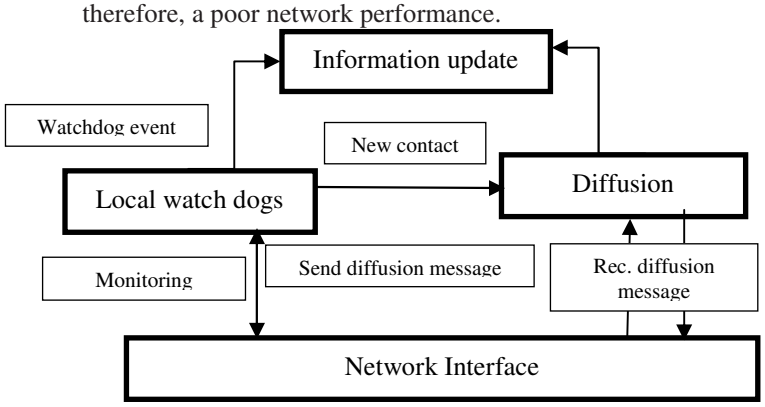
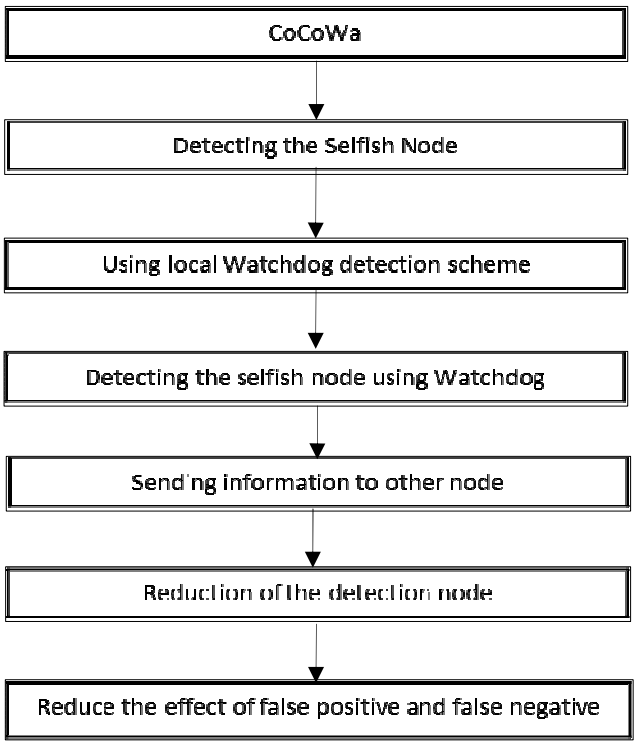


Fig 1: CoCoWa Architecture

The Local Watchdog has two functions: the detection of selfish nodes and the detection of new contacts. The local watchdog can make the following events about neighbour nodes:

PosEvt(positive event) when the watchdog discovers a selfish node for detecting, Negev (negative event) when the watchdog discovers that a node is not selfish for detecting, and NoDetEvt (no detection event) when the watchdog does not have enough information about a node (for example if the contact time is very low or it does not eavesdrop enough messages). The detection of new contacts is based on locality packet overhearing; thus, when the watchdog listens to packets from a new node it is expected to be a new contact, and so it makes an event to the network information module. The Diffusion module has two functions: the programme as well as the greeting of positive (and negative) detections. A key issue of our approach is the diffusion of information. As the number of selfish nodes is low compared to the total number of nodes, positive discoveries can always be conveyed with a low overhead. However, transferring only positive detections has a serious drawback: false positives can be spread over the network very fast. Thus, the diffusion of negative detections is necessary to neutralise the effect of these false positives, but sending all known negative discoveries can be troublesome, producing extreme messaging or the fast dispersal of false negatives. Subsequently, a negative diffusion factor (g) that is the ratio of negative detections that are essentially conveyed is used. This value ranges from 0 (no negative detections are transmitted) to 1 (all negative detections are transmitted).

III. STEP BY STEP REPRESENTATION FOR DETECTING SELFISH NODE



IV. TRUST BASED COCOWA ROUTING PROTOCOL

We incorporate our COCOWA along trust model with AODV routing protocol in order to prevent the malicious behavior and 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. 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
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. 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 with its trust value from which one with the maximum trust is selected it can transmit this information to it so, from that moment on, both nodes store information about this positive (or negative) detections. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative trans-mission 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. 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.

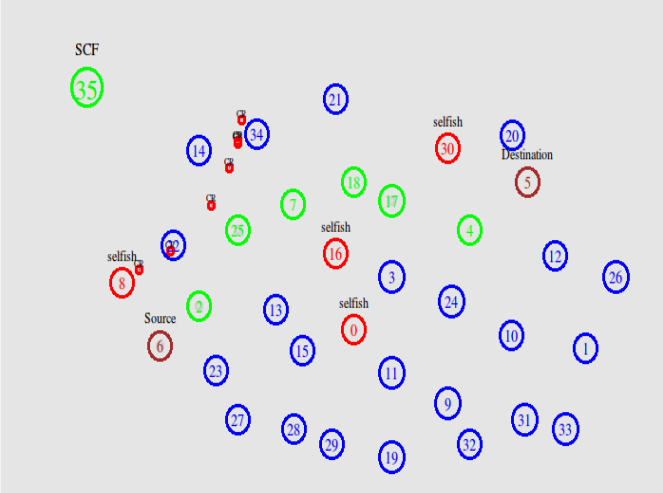


Fig 2 shows detecting the selfish node from the source to destination with security and clearing all the attackers.

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

Table 1: Packet format

The table 1 shows about packet format for the trusted model it shows that the type of node and fields of RADG. RREQID is route request ID to calculate message for sending actual message. If the messages are to calculate for the positive or negative event then send the reply message. 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 should be calculating for how long the message will send to destination in trust path.

V. SIMULATION TOOLS

Parameter	Value
No of Nodes	10 to 50
Area size	500 x 500
Mac	802.11
Radio range	250m
Simulation on time	50 sec
Traffic source	CBR
Packet size	512
Mobility model	Random way point
Speed	2 m/s
Pause time	10 sec
Channel data rate	2 mbps

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. 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.

VI. CONCLUSION

In this paper a novel approach CoCoWa is used as a collaborative contact-based watchdog to reduce the time and to improve the effectiveness of detecting selfish nodes. In addition, it is also used in reducing the harmful effects of false positives, false negatives and malicious nodes. In the proposed methodology, we detailed our COCOWA along trust model with AODV routing protocol in order to prevent the malicious node behavior and uniform utilization of network resources. The source pings the destination by sending a sample message to find out whether the destination sends the reply for the received message or not. At the arrival of the reply from destination, the actual message is sent through the path which has the maximum trust model. This model is used to detect the attackers, so

that it provides security while sending messages from source to destination.

REFERENCES

[1] 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**.

[2] Ashish Bagwari,Raman Jee,Pankaj Joshi,Sourabh Bisht "Performance of AODV Routing Protocol with increasing the MANET Nodes and its effects on QoS of Mobile Ad hoc Networks" International Conference on Communication Systems and Network Technologies **2012**.

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

[4]. Mishra and K. M. Nadkarni, "Security in wireless ad hoc networks – A Survey", in TheHandbook of Ad Hoc Wireless Networks, M.Ilyas, Ed. Boca Raton: CRC Press, **2002**, pp.**30.1-30.51**.

[5]. P. Papadimitratos and Z. Hass, "Securing Mobile Ad Hoc Networks", in The Handbook of Ad Hoc Wireless Networks, M. Ilyas, Ed. Boca Raton: CRC Press, **2002**, pp. **31.1-31.17**

[6] S. Marti, T. Giuli, K. Lai, and M. Baker, ―Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, Proc. MobiCom, Aug. 2000.

[7] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp.**1835–1841**, Apr. **2008**.

[8] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf.Perform., Computer, Commun, pp. **747–752, 2004**.

[9] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf, pp. **75–78, 2003**.

[10] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Mo-biCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pages **255_265**, New York, NY, USA, **2000**. ACM.

[11] F. Kargl, A. Klenk, M. Weber, and S. Schlott, "Sensors for detection of misbehaving nodes in MANETs," in Proc. Detection Intrusions Malware Vulnerability Assessment, pp. **83–97, 2004**.

[12] Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in Proc. IEEE Conf. Comput. Commun, pp. **857–865, 2010**.

[13] Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," IEEE Trans. Veh. Technol., vol. 60, no. 5, pp. **2224–2238**, Jun. **2011**.

[14] M. Mahmoud and X. Shen, "ESIP: Secure incentive protocol with limited use of public-key cryptography for multihop wireless networks," IEEE Trans. Mobile Comput., vol. 10, no. 7, pp. **997–1010**, Jul. **2011.**

Author Profile

Dr.G.Satyavathy received her MCA and MPhil Degree in Computer Science from Bharathiar University and Bharathidasan University, India in 1999 and 2005 respectively. She received her doctorate degree in Computer Science from Anna University, India in the year 2014. Currently, she is an Assistant Professor in the department of Computer Science, Sri Ramakrishna College of Arts and Science for Women, Coimbatore, India. Her Research interests are in the area of Networking, Image Processing, MANET.

P.Anitha received her M.B.A and M.C.A Degree from Bharthiar University, India in the year 2013 and 2014 respectively. She is pursuing her Master of Philosophy (M.Phil) in Computer Science at Sri Ramakrishna College of Arts and Science for Women, Coimbatore, India. Her area of research interests include Networking and MANET.