A Secure Message Exchange and Anti-Jamming Mechanism in MANET

S Sevvanthi[1] G Arul Kumaran[2]
[1,2]Department of Information Technology
[1,2]Vivekanandha College of Engineering for Women

Abstract— Secure neighbor discovery is the fundamental process in the MANET deployed in aggressive environment. It refers to the process that nodes exchange messages to discover and authenticate each other. It is defenseless to the jamming attack in which the adversary intentionally transmits signals to prevent neighboring nodes from exchanging messages. Existing anti-jamming communications depends on JR-SND. The JR-SND, a jamming-resilient secure neighbor discovery scheme for MANETs based on Random spread-code pre-distribution and Direct Sequence Spread Spectrum (DSSS). In Existing, they prevent the jamming and introduce the anti-jamming mechanism using DSSS introduce the secure message exchange mechanism and prevent the collisions during packet transmission. But in this we lack of introducing to detect the selfish and malicious nodes in the network. For this, in the Future Work we will enhance the work by detecting the selfish nodes using Watchdog and Neighbor Coverage-based Probabilistic Rebroadcast Protocol (NCPR).
Key words: MANET, NCPR

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are auspicious area based on the ability to self-configuring mobile devices connection into wireless network without using any infrastructure. MANETs are mobile; they use wireless connections to connect to various networks. In the occasion where there is a group effort required, the MANETs plays a major role in wireless communication and provides effective communication.

SECURE neighbor discovery is a fundamental functionality in mobile ad hoc networks (MANETs) deployed in aggressive environments. It refers to the process that nodes exchange messages to discover and authenticate each other [2]. Therefore the basis of other network functionalities such as medium access control and routing, secure neighbor discovery need be often performed due to node movability.

Direct Sequence Spread Spectrum (DSSS) is a common forms of spread spectrum techniques [15]. In classic spread spectrum techniques, senders and receivers need to pre-distribute a secret key, with which they can generate spread codes, for communication. If a jammer knows the secret key, the adversary can easily jam the communication by the spread codes, used by the sender. There have been a few current attempts to remove the circular dependency of jamming-resistant communications on pre-shared keys like JR-SND [1]. Many existing protocols in MANET work properly only against single node attacks. They cannot provide protection against multiple malicious nodes working in collusion with one another. Since packet transmission in MANETs depends heavily on mutual trust and cooperation among the nodes in the network, therefore determining the trust of an individual node before actually forwarding packet to it becomes essential for successful packet transmission.

In this paper we propose, Watchdog timer and NCPR can help in detecting malicious behavior of some nodes in the network. The NCPR is used to decrease routing overhead based on neighbor coverage knowledge and rebroadcast probability (NCPR) [13]. The excess of route request has been decreased using several methods like neighbor coverage based probabilistic (NCPR) method which guides to high end-to-end delay and packet delivery ratio. The node which has sufficient power to send the packet is recognized by using good neighbor node detection method. Here, This NCPR provides optimal solution for finding good nodes. Performance metrics in classification of nodes are transmission range and power of node, signal strength, high packet forwarding capacity and relative location of node.

Our main contributions are summarized as follows.

1) We identify selfish node in MANETs as a related problem that cannot be addressed by existing anti-jamming techniques such as
2) We propose a NCPR and Watchdog scheme to detect node behaviour.

The rest of this paper is structured as follows. Section II discusses about the related work. Section III introduces the proposed scheme. Section IV illustrates the implementation of proposed system. Section V presents the performance evaluation and Section VI concludes this paper.

II. RELATED WORK

Several schemes have been proposed to enable two nodes to establish a secret spread code (or key) under the jamming attack. The schemes proposed in [1] are all based on DSSS and a publicly known spread-code set and thus vulnerable to the DoS attack. In [7], proposed a scheme, Mobile Secure Neighbor Discovery (MSND), which offers a measure of security against wormholes by allowing participating mobile nodes to securely determine if they are neighbors. In [3], proposed an enhanced security scheme against jamming attack with AOMDV routing protocol [4]. The jamming attacker delivers huge amount of unauthorized packets in the network and a result network gets attained. The proposed scheme identifies the jamming attacker and blocks its activities by identifying the unauthorized packets in network. Multipath routing protocol AOMDV is used to improve the network performance but there is a state that jamming phase occurs naturally and is not achieved by attacker intentionally [5]. In presence of attacker security method always provides the secure path and through multipath routing the possibility of secure routing is enhanced. The schemes proposed in [1] and [6],[13] are all based on DSSS. DSSS is a modulation technique widely used in code division multiple access (CDMA) systems, e.g., IS-95. In a DSSS system, the sender spreads the data signal by increased it by an independent noise signal known as a spread code, which is a pseudorandom sequence of 1 and -1 bit values at a frequency much higher than that of the

original signal. The energy of the original signal is thus spread into a much broad band. The receiver can modulate the original signal by multiplying the received signal by a synchronized version of the same spread code, which is known as a de-spreading process. To transmit a message, the sender first transforms the message into a NRZ sequence by replacing each bit 0 with -1 and then multiplies each bit of the message by a spread code to get the spread message also known as the chip sequence [1]. In [4], Proposed an method, use passive ad hoc identity method and key distribution. Detection can be done by a single node, or multiple trusted nodes can join to improve the accuracy of detection. In [4] Sybil attacks pose a great threat to decentralized systems like peer-to-peer network and geographic routing protocols. More recently, In [9] proposed an anti-jamming scheme that explores interference cancellation and transmit precoding capabilities of MIMO technology.

III. PROPOSED SCHEME

This System proposes a scheme is watchdog and rebroadcast delay. The rebroadcast delay is to determine the forwarding order. The node which has many common neighbors with the previous node has the lower delay. If this node rebroadcasts a packet, then many common neighbors will know this fact. Therefore, this rebroadcast delay enables the information that the nodes have transmitted the packet spread to many neighbors. This is performed by using the Neighbor Knowledge Probabilistic Rebroadcast Protocol based on the neighbor knowledge method. And the watchdog can be used to detect the selfishnode while the packet transmission.

IV. IMPLEMENTATION

A. Watchdog

Watchdogs are well known mechanism to detect the attacks from selfish nodes in the network. A way to decrease the overall detection time of selfish nodes in a network is the collaborative watchdog. Collaborative contact means both nodes are coordinate then if one of them has one or more positive. It can transmit information to other nodes. The nodes can directly communicate with each other if a contact occurs (that is, if they are within communication range). Supporting this coordination is a cost intensive activity for nodes [12]. Thus, in the real world, nodes could have a selfish behaviour, being unwilling to forward packets for others. Selfishness means that nodes decline to forward other node packets to save their own resources. Therefore, detecting such nodes quickly and accurately for the overall performance of the network. Previous works have showed that watchdogs are appropriate mechanisms to detect misbehaving and selfish nodes.

B. NCPR (Neighbor Coverage-Based Probabilistic Rebroadcast Protocol)

The proposed scheme is a Neighbor Coverage based probabilistic Rebroadcast protocol that can be used to decrease routing overhead based upon neighbor coverage knowledge and rebroadcast probability. The overhead of route request has been reduced using several methods like (NCPR) neighbor coverage based probabilistic method which guides to high end-to-end delay and packet delivery ratio. The node which has sufficient power to transmit the packet is identified by using good neighbor node detection method. This method provides best solution for finding good nodes. Performance metrics in categorization of nodes are transmission range, power of node, high packet forwarding capacity and relative position of node.

Selfishness of the node is categorized as two:

- Full selfishness and
- Partial selfishness.

1) Full Selfishness:

The node which cannot be able to transmit and also receive the data packets in the network.

2) Partial Selfishness:

The node which has ability to receive the data packets and cannot able to transmit the data packets.

C. Algorithm Description

The legal description of the Neighbour Coverage based Probabilistic Rebroadcast (NCPR) for decreasing routing overhead in route discovery is shown in algorithm

1) Definition:

RREQv: RREQ packet received from node v. Rv.id: The unique identifier of RREQv. U(u, x): Uncovered neighbours set of node u for RREQ whose id is x. N(u): Neighbour set of node u. Timer(u, x): Timer of node u for RREQ packet whose id is x. {Note that, in the actual implementation of NCPR protocol, every different RREQ needs a UCN set and a Timer.}

If n_i receives a new RREQs from s then
{Compute initial uncovered neighbours set $U(n_i,Rs.id)$ for RREQs:}
$U(n_i,Rs.id) = N(ni) - [N(ni) \cap N(s)] - \{s\}$
{Compute the rebroadcast delay $Td(n_i)$:}
$Tp(n_i) = 1 - [|N(s) \cap N(n_i)| / |N(s)|]$
$Td(n_i) = MaxDelay \times Tp(n_i)$
Set a $Timer(n_i,Rs.id)$ according to $Td(n_i)$
end if
while ni receives a duplicate RREQj from n_j before $Timer(n_i,Rs.id)$ expires do
{Adjust $U(n_i,Rs.id)$:}
$U(n_i,Rs.id)=(n_i,Rs.id) - [U(n_i,Rs.id) \cap N(n_j)]$
discard(RREQj);
end while
if $Timer(n_i,Rs.id)$ expires then
{Compute the rebroadcast probability $Pre(n_i)$:}
$Ra(n_i) = |U(n_i,Rs.id)| / |N(n_i)|$
$Fc(n_i) = Nc / |N(n_i)|$
$Pre(n_i) = Fc(n_i) \cdot Ra(n_i)$
if $Random(0,1) \leq Pre(n_i)$ then
broadcast(RREQs)
else
discard(RREQs)
end if

The node n_i receives an RREQ packet from its previous node s, it can use the neighbor list in the RREQ packet to calculate how much its neighbors have not been covered by the RREQ packet from s [13]. If node n_i has more neighbors unveiled by the RREQ packet from s, which means that if node n_i rebroadcasts the RREQ packet, the RREQ packet can reach more additional neighbor nodes. In algorithm N(s) and N (n_i) are the neighbors sets of node s and n_i, respectively. s is the node which sends an RREQ

packet to node n_i. When a neighbor receives an RREQ packet, it could calculate the rebroadcast delay Td (n_i) according to the neighbor list in the RREQ packet and its own neighbor list. Where Tp (n_i) is the delay ratio of node n_i, and MaxDelay is a little constant delay. | . | is the number of elements in a set. The node s sends an RREQ packet, all its neighbors n_i, i = 1,2 . . . | N(s)| receive and process the RREQ packet. If node n_i receives a replicate RREQ packet from its neighbor n_j, it knows that how many its neighbors have been covered by the RREQ packet from n_j. UCN set according to the neighbor list in the RREQ packet from n_j . After adjusting the U (ni), the RREQ packet received from n_j is disposed. When the timer of the rebroadcast delay of node n_i expires, the node obtains the final UCN set. Note that, if a node does not sense any duplicate RREQ packets from its neighborhood, its UCN set is not changed, which is the initial UCN set [13]. We define the additional coverage ratio (R_a (n_i)) of node n_i. R_a becomes bigger, more nodes will be covered by this rebroadcast, and more nodes need to receive and process the RREQ packet, and, thus, the rebroadcast probability should be set to be higher. Then, we can use 5.1774 log n as the connectivity metric of the network. So we assume the ratio of the number of nodes that need to receive the RREQ packet to the total number of neighbors of node n_i is F_c (n_i). The arrangement of network connectivity approaching 1, we have a heuristic formula: |N (n_i)| . Fc (n_i) ≥ 5.1774 log n. Then Combining the additional coverage ratio and connectivity factor, we obtain the rebroadcast probability P_{re} (n_i) of node ni. if the Pre (n_i) is greater than 1, we set the P_{re} (n_i) to 1. Note that the calculated rebroadcast probability P_{re} (n_i) may be greater than 1, but it does not collide the behavior of the protocol. It just shows that the local density of the node is so low that the node must forward the RREQ packet. Then, node ni need to rebroadcast the RREQ packet received from s with probability P_{re} (n_i).

V. Performance Evaluation

We perform several tests using the ns-2 simulator. In order to do this, we implemented a specific watchdog module for this simulator available at (http://safewireless. sourceforge.net/). Using this simulator allows us to test networks with a large number of nodes, changing the number of attackers and the mobility of them.

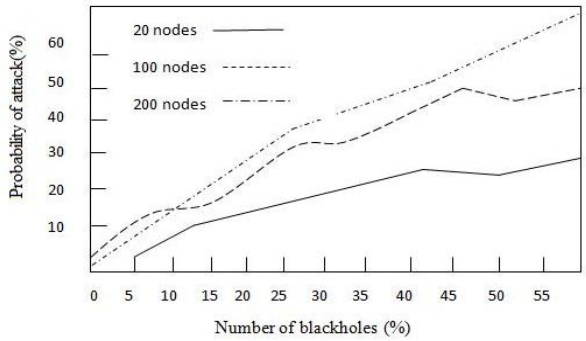

Fig. 1: Probability of an attack when varying the number of nodes and the percentage of attackers.

Figure 1 shows a preliminary study of how the percentage of malicious nodes and the total number of nodes of the scenario affects the probability that an attack is performed in a traffic flow. As we can see, not only the percentage of attackers affects the probability of found an attack in one test, also the number of total nodes of the scenario affects it. Afterwards we implemented the watchdog mechanism for this simulator and performed several tests varying the mobility of the nodes and the number of attacks to assess the effectiveness of the watchdog.

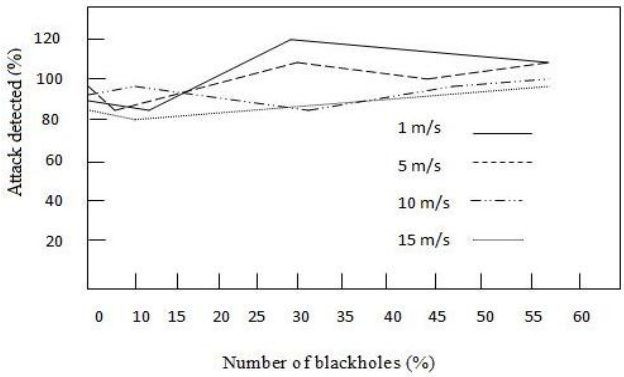

Fig. 2: Attacks detected by the watchdog

Figure 2 shows the results obtained with different parameters. We can see that mobility clearly affects the number of attacks detected. It decreases when mobility is increased. With a mobility of 1 m/s, near by 100% of the attacks are detected.

VI. Conclusion

In this paper, we propose watchdog mechanism to detect the selfish node based on NCPR. It refers to the process that nodes exchange messages to discover and authenticate each other. The results show that a collaborative watchdog can reduce the overall detection time of the selfish node. Thus improves the performance of the networks by avoiding these selfish nodes from the routing path. By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfishly.

References

[1] R. Zhang, Y. Zhang, and X. Huang, "JR-SND: jamming-resilient secure neighbor discovery in mobile ad-hoc networks," in IEEE ICDCS'11, Minneapolis, Minnesota, June 2015.

[2] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux, "Secure neighborhood discovery: a fundamental element for mobile ad hoc networking," IEEE Commun. Mag,vol. 46, no. 2, pp. 132–139, February 2008.

[3] Priyanka Sharma, Anil Suryawanshi, "Enhanced Security Scheme against Jamming attack in Mobile Ad hoc Network," IEEE International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), August 2014.

[4] P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan, "Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network, "International Journal of Communication and Computer Technologies Volume 02 – No.02 Issue: 02, Maech 2014.

[5] Vme-Rani Syed, Dr.ArifIqbal Vmar, Fahad Khurshid, "Avoidance of BlackHole Affected Routes in AODV BasedMANET," international Conference on Open Source Systems and Technologies (iCOSST), 2014.

[6] Q. Wang, P. Xu, K. Ren, and X.-Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," IEEE J. Select. Areas Commun., vol. 30, no. 1, pp. 16–30, 2012.
[7] R. Stoleru, H. Wu, H. Chenji, "Secure Neighbor Discovery in Mobile Ad Hoc Networks," IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, 2011.
[8] Marcin Poturalski, Panos Papadimitratos, Jean-Pierre Hubaux," Formal Analysis of Secure Neighbor Discovery in Wireless Networks," IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING, 2013.
[9] Qiben Yan, Huacheng Zeng, Tingting Jiang , Ming Li, Wenjing Lou, Y. Thomas Hou, "MIMO-based Jamming Resilient Communication in Wireless Networks," IEEE Conference on Computer Communications,2014.
[10] Liang Xiao, HuaiyuDai, Peng Ning, "Jamming-Resistant Collaborative Broadcast Using Uncoordinated Frequency Hopping," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol. 7, No. 1, February 2012.
[11] Chengzhi Li, HuaiyuDai, LiangXiao, Peng Ning, " Communication Efficiency of Anti-Jamming Broadcast in Large-Scale Multi-Channel Wireless Networks," IEEE TRANSACTIONS ON SIGNAL PROCESSING, Vol. 60, No. 10, October 2012.
[12] Reshma Lill Mathew, P. Petchimuthu, "Detecting Selfish Nodes in MANETs Using Collaborative Watchdogs," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.
[13] Lahari.P, Pradeep.S, "A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks,"International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014.
[14] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, Vol. 63, No. 9, November 2014.
[15] Shengli Zhou, Georgios B. Giannakis, Ananthram Swami, "Digital Multi-Carrier Spread Spectrum Versus Direct Sequence Spread Spectrum for Resistance to Jamming and Multipath," IEEE TRANSACTIONS ON COMMUNICATIONS, Vol. 50, No. 4, April 2002.

