International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

Detecting Malicious Entities in Wireless Mesh Networks

[1] K Vijay Kumar, [2] B Rasagna, [3] Prasad B
[1]II/IV, [2][3]Associate Professor
[1][2][3] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM) Hyderabad
[1] kudurutakavijay123@gmail.com [2] bheemarasagna@gmail.com [3]bprasad@gmail.com

Abstract: **Multi-hop wireless mesh networks provide a community with a communication infrastructure which gives the ability to have a single or few connections to the internet along with each other. The core philosophy is that each node in the network would route each other packets for the benefit of everyone in the mesh network. This can give rise to a malicious node taking advantage of the forwarding nature in the network. A malicious node can drop the packets that should be forwarded and only forward its own packets therefore decreasing the benefits of the network for nodes upstream from the "bad" node. We present a Random Tester Detection Protocol (RTDP) that will detect the malicious node. The protocol leverages the broadcast nature of wireless networks along with anonymous messages to detect the free riding nodes. The protocol is evaluated in a network simulator created using Java.**

Keywords: **Random Tester Detection Protocol, Multi-hop wireless mesh networks, Dissemination.**

I. INTRODUCTION

Cheating in multi-hop wireless mesh networks can have very negative effects on users of the network. Multi-hop wireless networks allow neighbors to connect their home networks together. There are many advantages to enabling such connectivity and forming a community mesh network. For example, when enough neighbors cooperate and forward each others packets, they do not need to individually install an Internet gateway but instead can share faster, cost-effective Internet access via gateways that are distributed in their neighborhood. Packets dynamically find a route, hopping from one neighbor's node to another to reach the Internet through one of these gateways. Another advantage is that neighbors can cooperatively deploy backup technology and never have to worry about losing information due to a catastrophic disk failure. A third advantage is that this technology allows bits created locally to be used locally without having to go through a service provider and the Internet. Neighborhood community networks allow faster and easier dissemination of cached information that is relevant to the local community [1]. In this network the internet access is not controlled by a central entity but by everyone in the neighborhood.

a. Cheaters

The multi-hop wireless mesh networks rely on the cooperation and interconnection of nodes to accomplish the common goal of internet access and communication. This requirement of cooperation can give rise to individual cheaters in the network. Examples where individual behavior can be in conflict with the system goal include free-riding in peer-to-peer file sharing networks [3], cheating in online games [4], ISP competition in Internet routing [6], and network congestion control [8]. These cheater nodes will behave selfishly even to the detriment of the other nodes in the network.

b. Routing

The lack of infrastructure and organizational environment of mobile ad-hoc networks gives special opportunities to attackers. The opportunities we focus on in this paper deal with the routing aspect of malicious behavior. Routing attacks such as [7]:

- No forwarding of control messages or data. (Gray hole problem)
- Route salvaging through rerouting to avoid a broken link, although no error has been observed.
- Lack of error messages, although an error has been observed.
- Unusually frequent route updates.
- Silent route change

c. Problem

We will refer to cheating in a multi-hop network as failure to forward packets for other nodes. Those nodes are consuming global resources, as bandwidth and energy, to

obtain a better service or by free-ride their own packets without sending the other nodes packets. A goal for such networks is to ensure the network providing fairness in the network. This paper introduces a solution to the routing layer "gray hole" problem in wireless mesh networks. The "gray hole" problem is when a user decides to drop packets that are to be forwarded. The malicious user can use different methods to drop packets, such as periodic drops or drops based on the packet's content i.e. information about the behavior of that node. If the node drops all others packets then it becomes a "black hole" [6].

d. Detecting a Cheater

A solution is to eliminate the free-riding through a distributed protocol. The protocol must be able to detect the cheater in the network. A prevention-only strategy only works if the prevention mechanisms are perfect, if not, someone can find out how to get around them [7]. We propose a protocol using the method of detecting cheaters in the network along with reacting to the cheater once detected. The Random Tester Detection Protocol (RTDP) takes advantage of the broadcast nature of wireless networks buy listening to the transmissions of possible cheater nodes. This is accomplished through using each node in the network to check on the actions of other nodes. A node will randomly test its neighbors to detect if they are cheating. This is further described in section 3. The rest of the paper is organized as follows. The rest of this paper is organized as follows. Section 2 describes related work followed by Section 3 which describes RTDP protocol. Section 4 discusses the implementation of the protocol and the simulation results from the evaluation of the protocol. Section 5 discusses our conclusions. And finally Section 6 and 7 presents our future work and references.

II. RELATED WORK

Previous work in preventing network routing attacks has identified two areas of vulnerabilities, the route establishment and packet forwarding of the network. In route establishment, attacks such as route disruption, route diversion, and creation of incorrect states can degrade the quality of service of the network [6]. While in packet forwarding attacks, nodes will selectively drop some or all packets that should be forwarded, with the purpose of increasing the nodes throughput or decreasing the packet delivery ratios of other nodes.

2.1. Detection

The common characteristic among many solutions is a detection and reaction to the possible cheating node. Detection of the malicious node must happen first in order to take corrective action. Zhang and Lee [10] proposed intrusion detection for wireless ad-hoc networks to complement intrusion-prevention techniques. The authors describe a protocol using statistical anomaly-detection approaches and integrating intrusion detection information from several networking layers. They use a majority voting mechanism to classify behavior by consensus. A hop-by-hop checksum verification has been proposed [7]. The checksum is verified at each router to isolate a packet-corrupting router. Michiardi and Molva, proposed CORE, a collaborative reputation mechanism which uses a reputation mechanism that differentiates between subjective reputation (observations), indirect reputation (positive reports by others), and functional reputation (task-specific behavior), which are weighted for a combined reputation value that is used to make decisions about cooperation or gradual isolation of a node [11]. A suggested network management tool that monitors routers and networks in an autonomous system can be used to debug problems, control routing, and find computers that violate protocol standards [8]. A problem with this method is that a network management tool cannot be used to monitor all of the traffic in a network [11], and therefore they cannot be used to detect all bad routers.

2.2. Reaction

The second phase of the securing networks from malicious users is the reaction phase. This phase determines how the network will respond to the cheating node. Enforcement and incentive based schemes have been suggested as solutions combat the malicious node. Enforcement based schemes use mechanisms that discourage free-riding through the fear of punishment. Mahajan and Rodrig [2] describe their Catch protocol as using peer nodes (testers) to test the other nodes (testee) in the network. The isolation of a testee is decided by all testers in parallel. Each maintains a small history of per-epoch (statistical tests) test results, represented as a three state finite state automaton (FSA) that moves to the right when an epoch fails and the left when an epoch passes. If the FSA falls off the right edge, the testee is isolated, meaning no packets are forwarded to that node. The Confident protocol [9] uses a reputation system that is exchanged between neighbors along routes. If a node is detected as a bad, a label of Black sheep is attached to that node and other nodes will avoid using it for routing. Incentive-based approaches discourage free-riding by making cooperation more attractive. Nodes accumulate virtual currency by forwarding for others, which they can then use for sending their own packets. One such protocol introduced nuglets, where a security module maintains a counter, called nuglet counter, which is decreased when the node wants to send a packet as originator, and increased when the node forwards a packet. The value of the nuglet counter must remain positive, which means that if the node wants to send its own packets, then it must forward packets for the benefit of other nodes [13]. In priority forwarding [12] also uses a similar scheme, using virtual currency. These schemes rely on a trusted central authority or tamper-proof hardware to ensure the integrity of the currency, and to redistribute wealth so that

even nodes that are not in a position to forward for others can send their packets.

III. RTDP

The RTDP protocol provides the ability to detect nodes in a wireless mesh network attempting to free ride. The protocol makes a few assumptions about the condition of the network:

- A-priori route establishment: A node knows the next hop for all destinations along with knowledge of all its 1-hop neighbors.
- Single Malicious Nodes: "bad" nodes act alone (selfish).
- Each node has a unique identity.
- Each node randomly sends data to destinations.

3.1. Detection Issues

Problems arise in the detection of free riders performing "gray hole" attacks in a wireless mesh network. One problem is that of a node must determine the difference between a node dropping packets because of common transmission loss in a wireless environment or as an attempt to give priority to its own packets. This fact would require a solution that would be resistant to the effects of packet transmission loss. A second problem is a malicious nodes detection of packets that are intended to identify, limit, or notify the bad user's intentions. Because a wireless mesh network requires data to be forwarded by nodes in the network along with the broadcast nature of the transmissions, a malicious node could possibly detect a packet that was sent in reference to its behavior. RTDP uses anonymous challenge messages and takes advantage of the broadcast nature of wireless networks to address these problems [2]. These anonymous messages cannot be detected by a free riding node.

3.2. Testing Decision

In RTDP a node can be in two states; either testing or not. Each node in the network will test all of its neighbors through the sending of anonymous messages as described in Section 3.3. A node decision to test a neighbor node is based on the amount of messages that are sent to that node. We will refer to the node performing a test as a tester and the node being tested as testee. When the number of messages from a tester to a testee reaches a specified number TT(testing trigger) the tester sends a test message to the testee. The testing trigger number can be randomly chosen or explicitly defined, but varying this number increases the anonymity of the challenge packets. For every neighbor node the amount of sent messages are counted. Sent messages include those that are originated or being forwarded by the node.

3.3. Anonymous Messages

When a node decides to test one of its neighbors the tester will send out an anonymous message to that node, called a challenge packet. In order to maintain the anonymity of the packet, almost any packet can be used as a challenge packet. For example, a challenge packet could be a packet that the node itself generates or a packet that it is forwarding from another source to the testee. This would make it impossible for the testee node to know which packet is being used for testing. There is one restriction on the choice of challenge packets, it must be destined to another node that is not currently being tested but must have the current testee as its next hop. The node will utilize the broadcast nature of wireless networks by listening to the retransmission of the packet, called query packet, by the testee to its next hop and will copy the retransmitted message. Comparing the query packet to the challenge packet the testee will decide the malicious activity of the testee node as described in the next section.

```
While(1)
{ For(all neighbors)}
Count packets to be forwarded by neighbor;
If(count reaches the testing trigger) {
++challenge_count; find suitable challenge
packet from queue; if(suitable packet found)
}
Challenge packet = suitable packet;
}
else {Create challenge packet}
store contents of challenge packet;
Place challenge packet in front of queue;
}
Listen to retransmissions of testee; If(challenge
packet is retransmitted)} ++successful_count;
}
CI= successful_count / challenge_count;
```

Fig 1: Pseudo code of RTDP

3.4. Free Rider Decision

Once a node is chosen to be tested by a tester, a challenge packet is sent and its retransmission is captured. The testee's retransmission packets are cached in the tester. Caching is needed because a testee node will be sending out packets according to its packet queue. The amount of retransmission packets that are cached are determined by the node degree, amount of neighbors, of the network. A greater node degree will result in higher number of packets that needs to be cached. Each cached packet is checked for a match to the challenge packet. Each successful retransmission is recorded for each testee. The number of sent challenge packets is known by the tester and this number is divided into the number of successful retransmissions. The confidence index (CI) is the resulting number, Figure 2 shows the calculation.

for $\forall$ $\eta_i = \frac{\#\text{ of successful retransmission}}{\#\text{ of challenge packets}} = CI_i$

where η_i = # of nodes and CI_i= confidence index for each node

The CI statistic gives an insight to the percentage of packets that are being dropped by a malicious user. The acceptable value would be determined by the network administrator. Figure 2 is a table that represents the different statistics of the CI and suggestions for the behavior of the testee node. The CI statistic is invariant of the packet loss from transmission errors. This lends from the fact that the retransmissions of the challenge packets are transmitted at the same rate as all the testee's packets along with the fact that the sending of challenge packets are randomly chosen. RTDP improves its detection of the free riders through the increasing iterations of the CI. This scheme addresses the two problems mentioned in Section 3.1, detection of negative information packets by free riders and mistaken identification because of packet loss due to transmission errors.

Confidenc	Comment
0.75-1.0	Testee is forwarding packets correctly
0.5-0.75	Testee is probably dropping packets (grey hole)
Below 0.50	Testee is definitely dropping packets (grey hole)
0%	Testee has become a black hole

Table 1: Confidence Index Values.

IV. EXPERIMENTAL EVALUATION

This section will describe the experimental evaluation of RTDP. A network was created using Net Beans IDE 5.5 a Java programming environment.

a. Goal

The object of the experiment was to create a simulated network where the RTDP protocol could be evaluated. Nodes in the network must be able to send and receive packets, along with having the knowledge of its neighbors. Nodes in the network should create packets containing information that will support routing and the evaluation of the protocol. The simulation should provide results that verify the performance of the protocol.

b. Simulation Network

A 5 node wireless mesh network was created to evaluate the RDTP protocol, Figure 3 displays this network. The network contained malicious users that drop other users' packets at varying rates. Each node in the network randomly chooses a destination, once chosen the node will send one packet to that destination. Node maintains the next hop information for all of the destinations in the network. Bad nodes will also generate it own packets, but when it is supposed to forward another nodes packet it will drop the packet according to set drop rate.

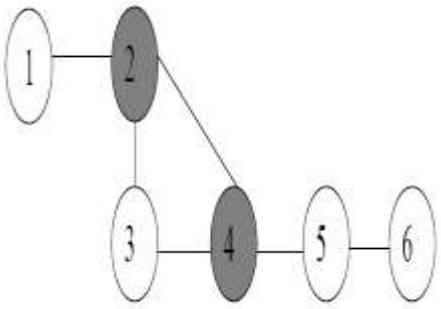

Fig 3: Simulated Network (grey nodes are "bad")

c. Bad Nodes Impact

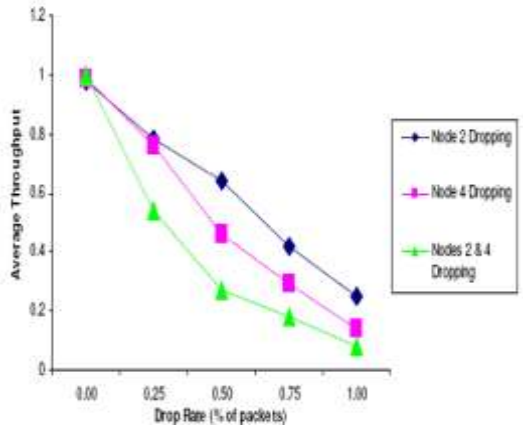

Fig 4: Effects of packet dropping

We first consider the impact that a bad node can have on the network performance. The average throughput of the nodes in the network was measured as function of the rate of dropping nodes. The calculation of the average throughput is done by averaging number of successful deliveries by "good" nodes in the network. The experiment consists of node 2 first dropping packets, then node 4 becomes the sole bad node, and finally both nodes are dropping packets. Figure 4 shows the results from the

experiment. The experiment results highlight the effects of having malicious users in the network.

The bad nodes behavior greatly affected the throughput of the network. When both nodes 2 and 4 are dropping packets the system throughput quickly become less than 50%. This throughput is unacceptable for a network to function correctly. A second result of the experiment was demonstrating the great benefits seen by the malicious users. Figure 5 displays the throughputs of the bad nodes versus the average throughput of the rest of the network. The next section evaluates RTDP usefulness in detecting the cheating nodes.

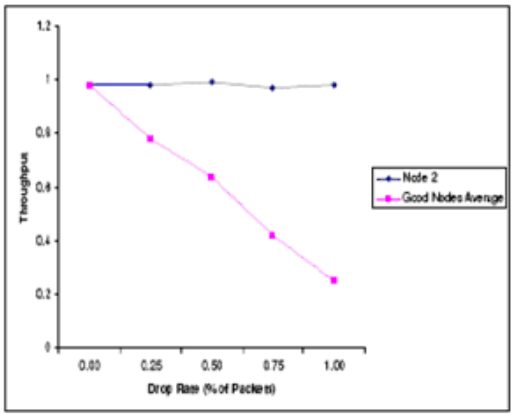

Fig 5(a): Throughput of "bad" nodes, (Node 2 Dropping)

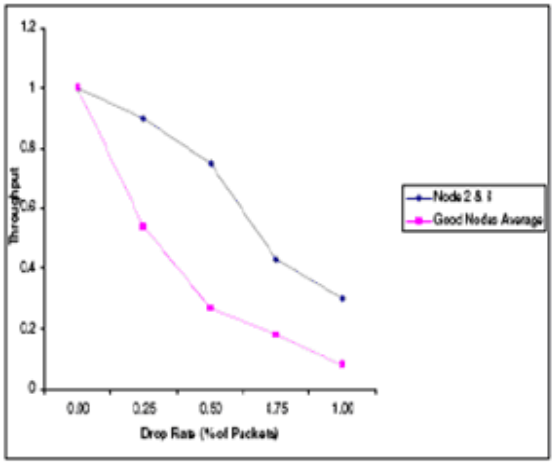

Fig 5(a): Throughput of "bad" nodes (Nodes 2 & 6 Dropping)

d. RTDP Evaluation

RTDP is evaluated by measuring the average CI for all of the nodes that are in position to test the "bad" node. A node is able to test another node if it is within 1-hop of the node. Table 2 shows a sample output for the program. In this simulation node 2 is the malicious user. We have varied the rate of dropped packets from node 2. Because of the randomness of the program nodes may not be tested by all possible testers.

Tester to testee	25%	50%	75%	100 %
Node 3 to Node 2	7/9	3/7	5/9	2/7
Node 3 to Node 4	9/11	2/7	8/9	10/10
Node 4 to Node 2	10/11	—	11/11	6/10
Node 1 to Node 2	11/11	8/8	9/10	1/9
Node 5 to Node 4	*111*	...	10/11	10/11
Node 2 to Node 4	11/11	2/11	8/8	—
Node 4 to Node 5	10/11	—	8/8	7/7

Table 2 : Node 2 Cheater (1 min simulation)

Figure 6 displays the number of challenge packets required until the average CI is with-in + or -10% of the actual drop rate. We set that the minimum amount of challenge packets needed to make a decision is 5.

These results show that the protocol was able to accurately detect the nodes that are dropping packets. For the 25% drop rate the detection is illusive because challenge packets may not get dropped by the "bad" node.

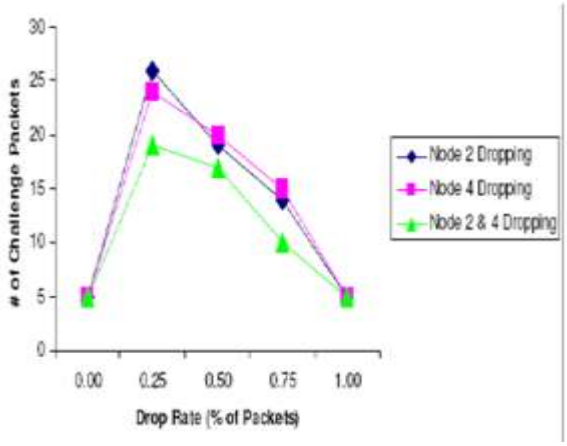

Fig 6: Number of Challenge packets needed

V.CONCLUSIONS

Multi-hop wireless mesh networks can provide great benefits to a community of users. In order for the network to function properly the cooperation of all members in the network

is required. Malicious users can cheat in this environment by dropping others packets and forwarding their own. We have presented the RTDP to detect these free riders in the mesh network. Unlike RTDP, previous suggested protocols rely on the use of centralized authorities to facilitate the policing of free riding nodes. A problem that arises in detecting malicious users is a node detecting that it is being identified as a cheater; the RTDP eliminates this problem through the use of anonymous messages. The protocol was evaluated using a Java based network simulator. In our experiments we showed that the protocol was able to detect the free riding nodes in the network. It was demonstrated that the CI statistic becomes increasingly accurate as the number of iterations of the protocol increases.

VI. FUTURE WORK

The next step is to implement a mechanism to react to a detected malicious user. This would be the natural progression of the protocol. In order to successfully stop or hinder the cheater's ability to affect the network both detection and reaction is needed. A proper reaction is to isolate the cheating node from the network, meaning no packets are routed through the "bad" node. Reaction to a cheating node would involve multiple "good" nodes in the network. The nodes would collaborate by sending messages to each other about malicious nodes to facilitate an isolation decision.

REFERENCES

[1] M. L. Sichitiu. Wireless Mesh Networks: Opportunities and Challenges. http://www4.ncsu.edu/~mlsichit/Research/Publications/wwcChallenges.pdf

[2] R. Mahajan, M. Rodrig, D. Wetherall, J. Zahorian. Sustaining Cooperation in Multi Hop Wireless Network. Network Systems Design and Implementation (NSDI) 2005

[3] Q. Sun and H. Garcia-Molina. A selfish link-based incentive mechanism for unstructured peer-to-peer networks. In 24th International Conference on Distributed Computing Systems, Mar. 2004

[4] M. Pritchard. How to hurt the hackers: The scoop on Internet cheating and how you can combat it. http://www.gamasutra.com/features/20000724/pritchard pfv.htm, July 2000

[5] L. Butty, J.P. Hubaux. Security and Cooperation in Wireless Networks. Thwarting malicious and selfish behavior in the age of ubiquitous computing. A graduate textbook, Draft Version 1.0 August 2, 2006

[6] S. Floyd and K. Fall. Promoting the use of end-to-end congestion control in the Internet. EEEE/ACM Transactions on Networking, Aug. 1999

[7] K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, R.A. Olsson. Detecting disruptive routers: a distributed network monitoring approach. Network, EEEE. Volume 12, Issue 5, Sept.-Oct. 1998 Page(s):50 – 60

[8] J. Case, M. Fedor, M. Scho_stall, and J. Davin. A Simple Network Management Protocol (SNMP)", May 1990. RFC 1157

[9] S. Buchegger, J.Y. Le Boudec. Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes I Fairness In Dynamic Ad-hoc Networks. 1C Technical Report IC/2002/01

[10] Y. Zhang, W Lee. Intrusion detection in wireless ad-hoc networks. In Proceedings of MOBICOM 2000, pages 275-283, 2000

[11]P. Michiardi and R. Molva. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia., 2002

[12]B. Raghavan, A. C. Snoeren. Priority Forwarding in Ad Hoc Networks with Self-interested Parties. University of California, San Diego.