Cross-layer Analysis for Detecting Wireless Misbehavior

Jim Parker Anand Patwardhan Anupam Joshi

Computer Science and Electrical Engineering Department
University of Maryland Baltimore County
Baltimore, MD 21250
{jparke2, anand2, joshi}@cs.umbc.edu

***Abstract*— Intrusion Detections Systems(IDSs) in ad hoc networks monitor other devices for intentional deviation from protocol, i.e., misbehavior. This process is complicated due to limited radio range and mobility of nodes. Unlike conventional IDSs, it is not possible to monitor nodes for long durations. As a result IDSs suffer from a large number of false positives. Moreover other environmental conditions like radio interference and congestion increase false positives, complicating classification of legitimate nodes and attackers.**

We present a scheme that helps in accurate diagnosis of malicious attacks in ad hoc networks. Our scheme employs cross-layer interactions based on observations at various networking layers to decrease the number of false positives. Our simulations show that our scheme is more effective and accurate than those based on isolated observations from any single layer.

I. Introduction

Mobile ad hoc networks (MANETs) are comprised of a dynamic set of cooperating peers, which share their wireless capabilities with other similar devices to enable communication with devices not in direct radio-range of each other, effectively relaying messages on behalf of others. Conventional methods of identification and authentication are not available, since the availability of a Certificate Authority (CA) or a Key Distribution Centre (KDC) cannot be assumed. Consequently, mobile device identities or their intentions cannot be predetermined or verified.

Communication protocols are though designed for fairness in contention resolution provide no enforcement mechanism to ensure it. Protocols are fair to the extent to which the devices conform to the protocol specifications. Wireless Medium Access Control(MAC) Protocols like 802.11 that employ distributed contention resolution for gaining access to the shared wireless channel are susceptible to attack from selfish nodes trying to gain an unfair share of the medium.

The various networking layers from the lowest physical layer to the application layer were designed for with the tacit assumption that devices comprising the network will be protocol conformant.

Herein lie several security threats, some arising from shortcomings in the protocols, and others from the lack of conventional identification and authentication mechanisms. These inherent properties of ad hoc networks make them vulnerable, and malicious nodes can exploit these vulnerabilities in the networking layers for selfish or even malicious motives. Selfish nodes can slightly deviate from the MAC protocol specification for contention resolution in order to gain an unfairly large share of the bandwidth. More harmful attacks like packet dropping, routing disruption, jamming attacks or other forms of Denial-of-Service (DOS) at any of the networking layers can severely disrupt MANET communications.

Traditionally, intrusion detection involves looking at events and activities in individual layers of the modeled OSI stack. Various pattern matches at the Transport layer, for example, can indicate SYN attacks.

However, sophisticated attacks that simultaneously exploit vulnerabilities at multiple layers of the communication protocols will be especially hard to detect. By using observations of both external and internal events at multiple layers of the OSI our approach will be to use observations both external and internal from various layers of the OSI stack for a more accurate evaluation of bad nodes and good nodes. In this paper we show the results of looking specifically at malicious RTS activity in the 802.11 MAC layer when combined with packet dropping at the Network layer.

Robust IDS and response systems will depend on accurate classification of attacks and identification of attackers. In order for devices to establish and maintain trust relations – and evolve reputations, there is a need to balance the intrusion detection effort with the individual node's primary function. The goal is to maximize the probability that malicious behavior will be correctly detected (True Positives), while minimizing the probability that good nodes will be falsely accused (False Positives).

II. Related Work

Several schemes including game theoretic models [3] that deter selfish behavior and misbehavior-resilient backoff algorithms [5] have been proposed to ensure fair sharing of the medium.

Other approaches include sender-receiver protocols by Kyasanur and Vaidya [6] and also by Cardenas *et al.* [4]. Kyasanur and Vaidya propose modification of 802.11 to integrate a receiver-initiated backoff penalty period built into the existing contention mechanism to ensure that selfish nodes cannot gain an unfair share of the bandwidth. Such schemes will help prevent unfair contention resolution, but will remain susceptible to attacks from colluding adversaries. Also, these schemes require changing the core MAC protocols themselves. Further, nodes that launch attacks at multiple networking layers will remain elusive. Malicious nodes seeking to disrupt traffic or to shape traffic can effectively use a DOS attack at the MAC level, that will go undetected at higher levels. In sufficient numbers such nodes may even be able to affect the routing process at the link level.

III. Proposed Approach

In previous work, we developed an intrusion detector (ID) for Mobile ad hoc networks (MANETs) in a GlomoSim simulation [7] and also deployed a prototype IDS on Linux-based handheld devices [8]. We assume the presence of symmetric omni-directional links within the ad hoc network. When a node that is not on the path from source to destination is able to hear transmissions of two intermediate nodes, A and B, that are on the *source route*, it becomes a snooping or *monitor* node for node B. Its ID function is to ensure that node B does not misroute, drop or alter the contents of the packet. The observing node records specific information fields contained in the packet p as it is inbound to intermediate node B and then compares those same fields with the information contained in packet p' as it is outbound from node B.

MANET traffic is comprised of packets being relayed from source to destination. An attacker can intentionally misroute, drop or mangle packets. In our previous work [8],we have shown how a combination of a secure routing protocol and an IDS can make a MANET resilient to such attacks. However, the IDS still suffers from False Positives because of several environmental conditions and properties inherent to wireless networks, viz., congestion, mobility and radio interference. Such false positives can be reduced by incorporating notions of proximity and congestion levels at neighboring nodes. Proximity can be determined by sensing the signal strength and response time of other nodes, whereas congestion can be detected by media contention and observed traffic throughput.

Heuristics are necessary for accurate diagnosis of various kinds of attacks, while ensuring that the device itself is not overwhelmed by the IDS effort. To make the IDS effort manageable we rely on a time-slicing threshold-based IDS scheme. This strategy is fairly effective because overtly disruptive attacks on data traffic can be easily detected by the IDS. Moreover, since the total throughput drops significantly in such attacks, the IDS needs to monitor fewer number of packets with increasing disruption.

To go undetected, the attacker must stay below the detection threshold, and is thus limited in his disruptive capability. However, a more sophisticated attacker may simultaneously exploit several vulnerabilities at multiple layers that do not match any single attack signature, and thus go undetected.

RTS attacks as well as attacks from other layers could go unrecognized with a single layer detection scheme. Our proposed approach to resolve problems is to combine input from all layers of the network stack to enable a more effective intrusion detection process. Here we present our first attempt by working with RTS/CTS input from the 802.11 MAC layer combined with network layer detection of dropped packets.

IV. Simulation

We used Glomosim 2.02 [10] to simulate a large scale deployment of a MANET with application nodes, malicious nodes, and software for intrusion detection on observer nodes. The simulation was restricted to a 150m x 150m for node placement and travel. 802.11 was chosen as the MAC layer protocol with each node having a communication range of approximately 30m; no fading model was used. Simulation time for each test was fixed to 300s and AODV was used as the routing protocol. We followed the same application traffic patterns used by Marti *et al.* [9], originally used by Broch *et al.* for performance comparisons of AODV and other routing protocols [2].

The application traffic consisted of 10 Constant Bit Rate (CBR) connections. Four nodes were sources of 2 CBR streams each, and two more nodes provided one CBR stream originating from each. Ten nodes, distinct from the sources, served as the endpoints for those 10 CBR streams (a slight variation from [2] where there are only 9 receiver nodes, one of them with two CBR endpoints). The data rate for each connection in the simulation was 4 packets/second, with a payload size of 64 bytes. CBR application traffic generated was the same for all tests.

The Random Waypoint Model was used to model movement of the all nodes, with a maximum speed of 5 m/s, minimum speed of 1 m/s, and maximum pause time of 15 seconds. A trace file generated by BonnMotion 1.1 [1] and used to specify the movement of individual nodes. Use of the trace file allows for result correlation between tests, since nodes take identical paths in each test.

By maintaining the same initial positions for the existing nodes, and the same mobility and traffic patterns, we studied the effect on neighbor table size, packets processed by IDS nodes, collisions, dropped packets, alarms generated, true positives, and false positives.

The total number of nodes for the tests was varied from 50 to 300, with malicious nodes increasing from 0% to 50% of total nodes in increments of 10 percentage points. In each simulation 25 nodes which were neither bad nodes nor traffic endpoints were designated to be observers – run the IDS. Bad nodes were configured to drop all data traffic yet participate correctly in the AODV routing process (gray holes). The bad nodes drop any traffic they are supposed to relay once included in the traffic path from sender to receiver. Additionally, in the simulations where RTS attacks were present, bad nodes generated RTS packets requesting 0.03 secs frequently enough to disrupt traffic.

The IDS nodes were configured with a threshold of 5 dropped packets over a 5 second interval. Alarms are raised if the threshold is exceeded. Post processing is done to classify the alarms into true positives (correctly identified malicious drops), and false positives (packets dropped for other reasons). Dropped packet data from the bad nodes is used for the classification.

RTS attacks were detected by observing nodes keeping track of the total requested duration in RTS packets over a 5 second period. A single node was observed to be requesting more than 50% of the bandwidth, was classified as an intrusion.

Three simulations were run. The first simulation had bad nodes dropping packets, with no RTS attacks. Alarms were raised for nodes observed to be exceeding the dropped packet threshold. The second simulation had bad nodes both dropping packets, and launching an RTS attack. The RTS attack was enough to disrupt traffic. As with the first simulation, alarms were raised based on observed dropped packets. The third simulation had bad nodes both dropping packets and launching an RTS attack.

V. Results

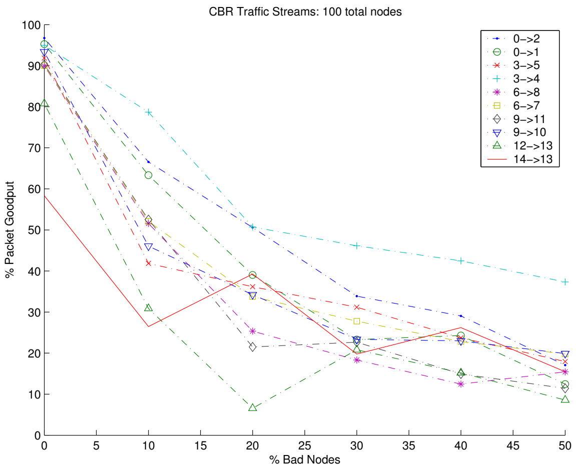

Fig. 1. CBR goodput

Figure 1 shows the percent of packets received for each of the CBR traffic streams as a function of the increasing percentage of bad nodes. As expected, the number of received packets decrease for each of the streams as the number of bad nodes running RTS attacks increase. The successful traffic throughput is being disrupted by malicious RTS requests that keep traffic off of the network. This was indicated by a decrease in the number of processed packets by the observer nodes as the number of bad nodes increase.

Data was collected by 25 observer nodes for each of the simulation runs. The same nodes acted as observers for each run with data being collected at 10 second intervals. The trends of the plots are much more important than the actual count numbers shown along the Y axis. The data for both plots reflect average true detection of malicious nodes over the total number of observers. So, for example, Figure 2 shows that during the run having 300 total nodes, with 50% of the nodes (150) acting malicious, all observer nodes put together detected on average about 15 bad nodes per observation interval. It should be noted that there is possible intersection between the observer node pools of detected bad nodes.

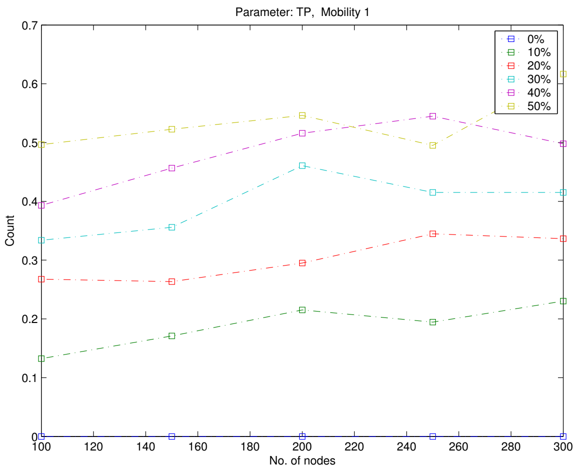

Fig. 2. Without RTS attack

Figure 2 shows True Positive results when the intrusion detection scheme is alarming on network layer packet drops. Notice that the positive results increase both as the total number of nodes increase and as the number of bad nodes increase.

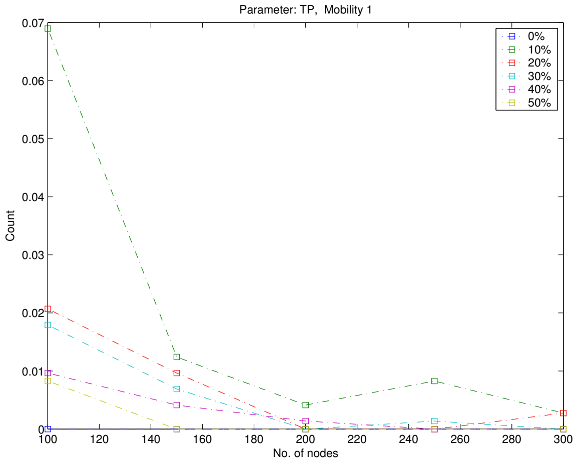

Fig. 3. With RTS attack

Figure 3 show True Positive results for packet drop alarms, but each bad node is also running an RTS attack. Notice that the positive results actually decrease as the total number of nodes increase and the number of bad nodes increase. Additional data from the simulation supports the fact that the RTS attacks diminished significantly the throughput of the CBR traffic. Therefore, without the CBR traffic being dropped by the bad nodes, there was a failure by the system to detect malicious behavior by the bad nodes.

The goal of the work is to compare the effectiveness of separate malicious detection schemes. In this case, we wanted to see how RTS attacks would effect our ability to detect malicious nodes dropping packets.

Our results showed that RTS attacks disrupted CBR application traffic almost to the point of denial-of-service. Due to the lack of application traffic, our malicious detection based on dropped packet observations failed to detect very little malicious activity. In other words, the malicious detection function showed nothing abnormal about the traffic and the RTS attacks would go undetected even as the application goodput goes to 0. It may be possible to combine the two malicious activities each having low rates to stay below thresholds, and disrupt traffic within the network.

At this point more simulation work is needed to correlate true and false positive results as they relate to identifying malicious nodes based on observed behavior.

VI. Conclusion

Combining observations from multiple layers provides more information on which to draw conclusions about whether a node is being malicious. Work on intrusion detection in MANETs has so far been restricted to diagnosing malicious behavior at a single layer or protocol. In this paper, we have presented an intrusion detection scheme that will use heuristics to classify intrusions by incorporating observed misbehavior from various levels of the protocol stack. This approach will help detect more sophisticated attacks that simultaneously target vulnerabilities in multiple layers to avoid detection.

It may be possible for either a sufficiently large number of malicious nodes or strategically located nodes to coordinate RTS/CTS attacks to influence formation of specific routing topologies conducive to their malicious motives. Such activity may occur selectively when bad nodes want important information channeled through one of their colluding nodes. That node could then change the information before forwarding. This is a more sophisticated scenario using a simple denial-of-service attack with RTS packets to create a favorable routing environment for the malicious nodes.

In our broader vision of IDSs for MANETs we plan to incorporate notions of relative proximity, mobility, congestion levels of neighboring nodes in order to reduce false positives. For instance, proximity can be estimated from signal strengths and response times. An interesting observation from our RTS attack simulation was that nodes launching an RTS attack would cause their neighbors to end up dropping packets, since the remaining nodes would fail to get a fair share of the bandwidth. Such nodes would otherwise be improperly classified as malicious.

References

[1] BonnMotion: A mobility scenario generation and analysis tool. http://web.informatik.uni-bonn.de/IV/Mitarbeiter/dewaal/BonnMotion, March 2005.

[2] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Mobile Computing and Networking*, pages 85–97, 1998.

[3] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux. On selfish behavior in csma/ca networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, pages 2513–2524, 2005.

[4] A. A. Cardenas, S. Radosavac, and J. S. Baras. Detection and prevention of mac layer misbehavior in ad hoc networks. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 17–22, New York, NY, USA, 2004. ACM Press.

[5] J. Konorski. Multiple access in ad-hoc wireless lans with noncooperative stations. In *NETWORKING '02: Proceedings of the Second International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; and Mobile and Wireless Communications*, pages 1141–1146, London, UK, 2002. Springer-Verlag.

[6] P. Kyasanur and N. H. Vaidya. Detection and handling of mac layer misbehavior in wireless networks. In *Proceedings of International Conference on Dependable Systems and Networks*, pages 172–182, 2003.

[7] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi. On intrustion detection and response for mobile ad hoc networks. In *Proceedings of the 23rd IEEE International Performance, Computing, and Communications Conference (IPCCC 2004)*, pages 747 – 752, Phoneix, AZ, USA, April 2004. IEEE Computer Society.

[8] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis. Secure Routing and Intrusion Detection in Ad Hoc Networks. In *Proceedings of the 3rd International Conference on Pervasive Computing and Communications*, pages 191–199, Kauai Island, Hawaii, March 2005. IEEE.

[9] K. L. S. Marti, T.J. Giuli and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of MOBICOM 2000, August 2000.*

[10] X. Zeng, R. Bagrodia, and M. Gerla. GloMoSim: A Library for Parallel Simulation of Large-Scale Wireless Networks. In *Workshop on Parallel and Distributed Simulation*, 1998.