Comparison of Two Intrusion Detection Schemes for Sparsely Connected Ad Hoc Networks

M. Chuah, P. Yang
{chuah, pey204}@cse.lehigh.edu
Department of Computer Science & Engineering
Lehigh University
Bethlehem, PA 18015

Abstract— **Several approaches have been proposed for intrusion detection in mobile adhoc networks. Most of the approaches assume that there are sufficient neighbors to help monitor the transmissions and receptions of data packets by other nodes to detect abnormality. However, in a sparsely connected adhoc network, nodes usually have very small number of neighbors. Using a traditional intrusion detection and mitigation scheme designed for well-connected adhoc networks, the delivery ratio in a sparsely connected ad hoc network (50 nodes over 2000x2000 m^2) can only improve from 76.5% to 79.9% with selective dropping attacks. Thus, we propose a ferry-based intrusion detection and mitigation (FBIDM) scheme for sparsely connected adhoc networks. Our simulation results indicate that our new ferry-based scheme is more effective than the traditional mitigation schemes that are used for well-connected mobile adhoc networks. Our FBIDM scheme reduces the impact of the data dropping attacks performed by malicious nodes in a sparsely connected ad hoc network. Without any mitigation scheme, the delivery ratio is 76.5% with selective dropping attacks. With FBIDM, the system achieves a delivery ratio that ranges from 87% (with a single ferry) to 93% (with four ferries) with selective dropping attacks. Without the mitigation scheme, the delivery ratio with blackhole attacks drops to 65.9%. With FBIDM, the achieved delivery ratio ranges from 82.9% (with a single ferry) to 91.9% (with four ferries) with blackhole attacks.**

Keywords-intrusion detection, routing, DSR, DoS resilience, sparsely connected adhoc networks, disruption tolerant networkst.

I. INTRODUCTION

An ad hoc wireless network is an autonomous self-organizing system of mobile nodes connected by wireless links where nodes not in direct range can communicate via intermediate nodes. A common technique used in routing protocols for ad hoc wireless networks is to establish the routing paths on-demand e.g. [1],[2]. On-demand routing protocols have been shown [3] to perform better than proactive link-state routing especially when there are many nodes that move at higher speed.

Security is critical in military ad-hoc networks since a disruption could lead to a loss of life. Thus, exchange of both control (e.g. route discovery) and topology update messages need to be authenticated and data packets need to be encrypted. Significant progress has been made in securing wireless routing protocols e.g. [4],[5],[6]. SEAD [5] uses one-way hash chains to provide efficient secure solutions for DSDV [7] while Adriane [6] uses a variant of Telsa [8] to provide source authentication for DSR.

All the above approaches suggest some solutions to provide secured communications in mobile ad hoc networks. However, the likelihood of authenticated devices being captured by the enemy in a chaotic battlefield environment is extremely high. Additional attacks can be launched by the adversary when he/she has full control of an authenticated device. For example, blackhole attacks can be launched where the compromised nodes participate in a routing protocol correctly and then drop all received data packets. Wormhole attacks [9] where two adversaries collude by tunneling packets between each other in order to create a shortcut in the network can be launched. In such attacks, the adversaries use low cost appearance to increase their chances of being selected as part of the route, and then attempt to disrupt the network by dropping all of the data packets.

Researches addressing the above category of attacks are quite scarce. Marti et al [10] attempted to address the survivability problem of the routing service when nodes selectively drop packets. They assume that trusted nodes monitor their neighbors. Links with an unreliable history are avoided in order to achieve robustness. The solution in [10] may not work well if nodes cannot hear their neighbors forwarding communications due to the use of different modulation schemes etc. In addition, in sparsely connected networks, there may not be enough neighbors that can act as trusted monitoring nodes. In [13], the authors attempt to apply intrusion detection techniques typically used in wired networks to ad hoc networks. They proposed that each node overhears all traffic its 1-hop neighbors sent so that it can compare currently observed values of some metrics, e.g. unconditional packet dropping ratio, selective random packet dropping ratio etc, with typical values observed in the past to detect abnormal behaviors. The intrusion detection approach [13] requires nodes to be in promiscuous mode and

process all overheard packets, thus it is rather energy consuming. In addition, the nodes may not hear its 1-hop neighbor's transmission due to power control and different modulation schemes. Furthermore, not enough neighbors can be used as monitoring nodes in sparsely connected networks.

There are several important scenarios where the ad hoc networks can be sparsely connected e.g. in battlefield scenarios, in vehicular ad hoc networks etc. In a sparsely connected ad hoc network, the existing intrusion detection scheme may not work since there may not be enough neighbors to monitor the packet transmission and reception processes. Thus, in this paper, we first evaluate the effectiveness of an intrusion detection scheme called ENDORSE [16] which is designed for well-connected mobile adhoc networks in a sparsely connected adhoc network environment where the nodes run the custodian transfer feature proposed for disruption tolerant networks [17]. Our results on malicious attack scenarios indicate that the performance of ENDORSE degrades with increasing network sparseness. Thus, we present a ferry-based intrusion detection and mitigation (FBIDM) scheme for sparsely connected *ad hoc* networks. Next, we present some simulation results that compare the performance of these two schemes in a sparsely connected adhoc network. Our results indicate that our ferry-based scheme is very effective for detecting malicious selective data dropping attacks in sparsely connected networks. With the FBIDM scheme, one can maintain high delivery ratio even in the presence of attacks from eight malicious nodes in a network with fifty nodes.

The rest of the paper is organized as follows: in Section II, we give some background on potential attacks in wireless ad hoc networks and some existing techniques that have been proposed for well-connected adhoc networks. We also describe their limitations when such techniques are applied to sparsely connected adhoc networks. In Section III, we describe a particular intrusion detection and mitigation scheme called ENDORSE which is designed for well connected mobile adhoc networks. In Section IV, we present our ferry-based intrusion detection and mitigation (FBIDM) scheme that is designed for sparsely connected adhoc networks. In Section V, we present some preliminary simulation results comparing the two schemes. In Section VI, we conclude with future work that we intend to explore.

II. BACKGROUND AND RELATED WORK

A. Related Work on Securing Ad Hoc Network

Attacks on ad hoc networks can be categorized as routing-disruption attacks, or resource-consumption attacks. Forging routing messages is one type of routing-disruption attacks. Normally, the routing messages are forged such that an attacking node is an intermediate node in a selected route and that attacking node can drop all or some of the data packets that it is supposed to relay. When all packets are dropped, such attacks are referred to as blackhole attacks. When only partial droppings occur, the attacks are referred to as gray hole attacks or selective dropping attacks. A wormhole attack occurs when a pair of colluded nodes linked via a faster network connection collaborate to get themselves elected to be intermediate nodes in a selected route and then launch gray hole or blackhole attacks. A rushing attack is a malicious attack that is targeted at on-demand routing protocols that use duplicate suppression at each node.

Several approaches have been proposed to secure ad hoc routing protocols. For example, Ariadne [5] protects source routing protocol such as DSR against a number of attacks. The authors propose a protocol to secure the route discovery phase and to ensure that all forwarded packets follow the same secure route. In [14], the authors propose a secure neighbor detection protocol to deal with rushing attacks. In their secure neighbor detection protocol, both the initiator and the responder can check if the other is within a maximum communication range. Packet leashes [9] have been proposed to deal with rushing attacks.The main idea is that by authenticating either an extremely precise timestamp or location information combined with a loose timestamp, a receiver can determine if the packet has traversed an unrealistic distance.

However, the above approaches will not work in Byzantine attacks where legitimate nodes can be compromised. Such nodes will participate correctly in the routing protocols. In addition, the above approaches also assume that the ad hoc network is relatively well-connected.

B. Byzantine Attacks And Existing Mitigation Techniques

Consider the case where a device or a set of devices could be compromised and be under the control of an adversary or set of adversaries that can collude. Once an adversary has control of an authenticated device, protocols which rely on authentication to provide security services become of little use. Attacks where the

adversary has full control of an authenticated device and can perform arbitrary behavior to disrupt the system are referred to as Byzantine attacks [11]. Authentication and data integrity mechanisms cannot protect against such attacks. Below, we elaborate on two Byzantine attacks that our two intrusion detection schemes attempt to address, and briefly describe some existing mitigation techniques that have been proposed to deal with such attacks:

a) Periodic drop attacks – An adversary node drops some or all packets periodically. When the adversary node drops all packets, the attacks are also referred to as blackhole attacks. The potential network damage caused by a blackhole attack is directly related to the likelihood of an adversary node being selected as part of the routing paths in a network. Thus, such attacks can be combined with other types of attacks e.g. rushing attacks to be more effective.

Existing proposed methods to deal with periodic dropping and blackhole attacks are discussed in [10],[11],[12]. The approach in [10[assumes that a node can overhear its neighboring nodes forwarding packets to other destinations. If a monitoring node does not overhear a neighbor forwarding more than a certain percentage of packets its needs to relay, then the monitoring node can conclude that its neighbor is adversarial. The solution in [10] may not work well if nodes cannot hear their neighbors forwarding communications due to different transmitted power levels. Secure Data Transmission [12] uses authenticated end-to-end acknowledgments from the infal destination to provide proof that the packets reached their destination. While it can detect the presence of a blackhole attack, it is unable to identify a specific compromised node along the path. ODSBR [11] uses end-to-end acknowledgments from the destination to detect the presence of a blackhole attack and then use an intelligent bisection probing technique to identify a faulty link within the path. The solution in [11] may incur huge overhead since they require that the destination returns an ACK for every packet sent by the source. its 1-hop. The intrusion detection approach in [13] requires nodes to process all overheard packets so that statistics about the received and transmitted packets can be maintained and compared to normal profile values to detect abnormaly. However, the nodes may not hear its 1-hop neighbors' transmission due to different transmission powers. In addition, there may not be many neighbors that can help to monitor any particular node for misbehaviors in sparsely connected networks.

(b) Rushing attacks – An adversary node propagates its modified flood packet to intermediate nodes before a flood packet reaches them through a set of valid nodes in an attempt to prevent a valid path from being established or increase its chance of being selected as part of the path. Typically when secure routing feature is used, an adversary node may not be able to modify the contents of flood packets but it can eliminate the extra delay that each node is required to wait before re-transmitting the flood to launch such attacks. Such attacks can be combined with the periodic data dropping or blackhole attacks to cause greater network damage.

In the rushing attack protection scheme discussed in [14], the nodes wait to receive up to k requests before randomly select one to forward. This solution may result in much network overhead because multiple rounds of communications are required for every hop the route request propagates. In [11], each node processes all duplicate flood packets and if a valid flood with lower metric is received, an additional rebroadcast is scheduled. However, such an approach consumes much energy since a node needs to process all duplicate flood packets.

To compare different detection/mitigation approaches, the following metrics can be used: (a) the packet delivery ratio, (b) control messages sent, (c) attack detection time, and (d) false positive/false negative rates. The first two metrics are typical metrics used to compare different routing protocols. An effective DOS resilience scheme should achieve higher packet delivery ratio with fewer control messages in the presence of the same number of malicious nodes. Intrusion detection time allows us to compare how fast an intrusion attack can be detected using different approaches. Any detection scheme should achieve low false positive and false negative rates. In this work, we only concentrate on the first two metrics.

In this paper, we deal with the two types of Byzantine attacks that we discuss in this subsection. Next, we describe an improved scheme called ENDORSE that we propose for mitigating such Byzantine attacks in well-connected ad hoc networks before we describe the ferry-based intrusion scheme that we design for sparsely connected ad hoc networks.

III. OVERVIEW OF ENDORSE

In ENDORSE [16], we use the following techniques: (a) traffic monitoring, (b) status reporting mechanism, (c) threshold-based corrective action, (d)

multiple path, and (e) onion encryption to combat the two attack types described above. In ENDORSE, during each observation window, each node monitors: (a) the number of packets per flow that it has received, (b) the number of packets per flow that it has forwarded.

In ENDORSE, a node only monitors traffic when it is in busy state (either receiving messages destined to itself or sending). No extra energy is spent on sniffing other traffic. In subsequent sections, we describe how we detect and mitigate data dropping attacks.

A. Detecting Dropping of Data Traffic

To determine if a node maliciously drops data packets, a monitor measures the number of packets it has sent to a 1-hop neighbor. Each source will periodically include a probe list in the data packets that it sends. The nodes in the probe list can be randomly chosen so that not every en route node needs to send a status report to the source. We can also use the method suggested in [11] to select nodes to be probed. A probed node only sends a status report periodically so it needs not send an ACK for every received data packet as described in [11]. Such probing mechanism is more energy efficient (fewer feedback packets) and allows a source to determine whether the packet loss in a particular route has exceeded a certain threshold and which link along the route is suspicious when such an event happens. Onion-style encryption as described in [11] is used to ensure that malicious nodes cannot modify the content of the probe list and probe responses. Each probed node will report a neighbor node that it monitors as malicious if that neighbor has consistently dropped 30% of the packets that it is supposed to relay. A source will conclude that a node is indeed malicious if it receives M bad reports about a particular node from other intermediate nodes. Corrective actions as described in the next subsection can be taken once a suspected malicious node has been discovered e.g. the source can use another route in the route cache that excludes the malicious node.

B. Threshold-based Corrective Action

When each source node receives bad reports about a particular node from M intermediate nodes, it will take two actions: (a) include the reported malicious node in its blacklist, (b) select another route either in the route cache or discovered via a new route discovery process that avoids the reported malicious nodes. Each source node will attach a blacklist that contain identities of all malicious nodes to its route request message, and hello messages so that these malicious nodes can be avoided in the route selection process.

C. Multiple Path Strategy

In ENDORSE, each node which is a destination can reply to the same route request max_replies of times. In addition, each node is allowed to probabilistically process duplicate flooded packets (say with probability p0) and when a valid request with a lower cost is found, a node can re-broadcast that duplicate route request. Thus, each source can find multiple paths to store in its cache even though it only uses one path at any time. When p0=1, our approach is similar to that described in [11].

D. Secure Routing/Onion-style Encryption

Any existing proposal on secure routing e.g. [4],[5],[6] [12] can be used in conjunction with the ENDORSE scheme to ensure that the contents of control messages like route request/route replies/route errors cannot be altered by malicious nodes. Similarly, spoofed control messages cannot be generated when any of the proposed secure routing approaches is used. Onion-style encryption is used to ensure that the probe list being sent by the source and the probe responses sent by intermediate nodes are not modified. The malicious nodes may drop probe request/response messages but then such actions would reveal their malicious behaviors and they will be detected.

IV. OVERVIEW OF FBIDM SCHEME

In our FBIDM scheme, we divide the geographical area into multiple cells and have ferries visit the center of each cell using some fixed routes as shown in Figures 1(a),(b) and (c) for the single ferry, two ferries and four ferries scenarios. Each ferry stops at a few locations within its route. At each location, the ferry will broadcast a secret service message that each destination knows how to decipher. Each destination will monitor the transmit sequence number (application layer) of any received packet and hence can determine the packet drop rate that it observes. If the packet drop rate observed by a destination exceeds a certain threshold, loss_threshold, then that destination will issue a unicast service request message to the ferry. The ferry will then travel to the destination and start probing the upstream nodes from the destination hop-by-hop to look for the malicious nodes. Intermediate nodes also monitor the packet lost rates. The ferry serves the service requests from different destinations using the first come first serve discipline. Once a ferry finishes servicing all the requests, the ferry will continue on its ferry route to look for future requests from other destinations.

The ferry keeps tracks of the percentage of packets that fails to be relayed by an intermediate node

as it travels around. If that percentage drops below loss_threshold (which is set to 30% in our experiments), then the ferry declares that node as malicious. Information of malicious nodes are attached in the secret service message that the ferry broadcasts as it travels along its route. Any node that hears such a broadcast will keep the identities of the malicious nodes in the blacklist that it maintains and not choose any of these nodes as custodians. Each node will store the messages until it can find a custodian that is not in its blacklist.

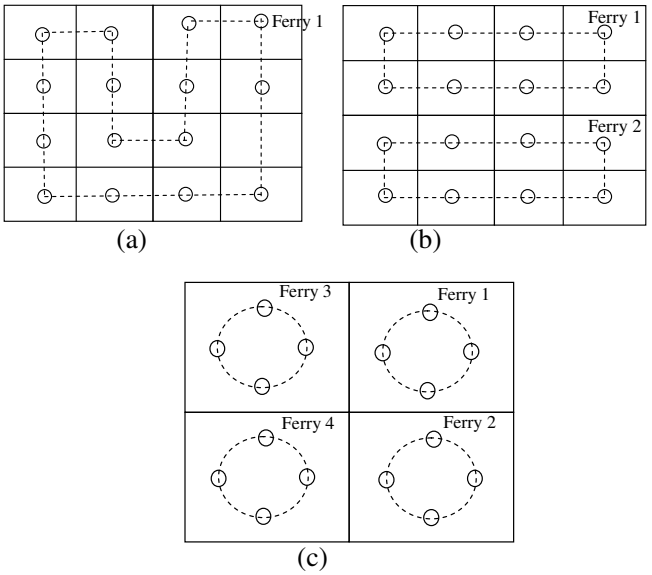

Figure 1: Ferry Routes for Intrusion Detection

V. SIMULATION STUDY

We have implemented both the ENDORSE and the FBIDM schemes in NS-2. IEEE 802.11 mac is used in our simulation. The simulated network consists of 50 nodes randomly distributed over an area of 2000x2000 m^2. The nodes move according to the random waypoint model with a maximum speed of 5 m/s and a pause time of 10 seconds. Unless otherwise stated, the ferry speed is 20 m/sec.

The routing protocol used is enhanced DSR (with custody transfer feature). In our earlier work [15], we have demonstrated that the custody transfer feature [17] helps to improve the delivery ratio in a sparsely connected ad hoc network. The custody transfer feature works as follows: accepting a message with custody transfer amounts to promising not to delete it until it can be reliably delivered to another node providing custody transfer or it arrives at the destination. Nodes holding a message with custody are called custodians. Normally, a message has a single custodian (referred to as sole custody) but in some circumstances, more than one custodian owns a message or message fragment (referred to as joint custody). We do not simulate message fragmentation so there is no joint custodian in our simulation. As for the traffic model, 10 CBR connections are used in our simulation experiments. The source and destination of the connections are chosen randomly. Each source generates 1 packet every second with a packet size of 512 bytes. The buffer size at each node is set to 600 messages.

The simulation time is varied according to each experiment since some warming up period is required for the monitors to generate normal profiles. Typical simulation time takes 5000 seconds. The metrics used in our experiments are (a) data delivery ratio, (b) extra overhead incurred for the intrusion detection and mitigation (IDM) scheme . The extra overhead is computed as the extra bytes that need to be transmitted as a result of running a particular IDM scheme over the total received bytes.

A. Results and Discussion

1) Effectiveness of the IDM schemes

In our first set of experiments, we introduce eight malicious nodes that drop 50% of the data packets they receive if they are chosen to be intermediate nodes for delivering any of the 10 data flows. The data packet generation rate is 1 pkt/s. For the ENDORSE scheme, the source sends probes every 500 seconds. The probes are piggybacked onto the data packets. Upon receiving a probe, an intermediate node reports the number of data packets it has received and forwarded between the last probing time and the current probing time. Upon receiving the reports from an intermediate node, the source node can calculate the packet delivery ratio for the intermediate node and decide if any malicious packet dropping occurs at that intermediate node. After sending out a probing request, the source node sets a probe response timer to wait for the status reports. If the source node does not receive the status reports from intermediate nodes after the timer expires, the source node will resend the probing request. The timer was set to 500 seconds after conducting some preliminary studies to find out how long it takes for intermediate nodes with similar node density take to return a probe response. Table 1(a) shows the results we obtain using ENDORSE and using the ferry-based intrusion detection and mitigation (FBIDM) schemes.

	With mitigation	Without mitigation	Without Attack
ENDORSE	79.9%	76.5%	99.6%
FBIDM	86.9%	76.5%	99.6%

Table 1(a): Delivery Ratio with the two IDM schemes.

Table 1(a) shows that without mitigation, the delivery ratio drops from 99.6% to 76.5%. With the ENDORSE scheme, the delivery ratio improves to 79.9% but with the FBIDM scheme, the delivery ratio improves to 86.9%. We also investigate the performance of the two schemes in a sparser network with 50 nodes distributed over 2500x2500 m^2 (Scenario 2) . The results for this new scenario is shown in Table 1(b). Without attack, the delivery ratio for this sparser network is 96.7% but with attack, the delivery ratio drops to 75%. FBIDM is able to improve the delivery ratio back to 83.3% but the ENDORSE scheme can only improve it to 77.2%.

	With mitigation	Without mitigation	Without Attack
ENDORSE	77.2%	75.0%	96.7%
FBIDM	83.3%	75.0%	96.7%

Table 1(b) Delivery Ratio for the two IDM schemes with Scenario 2

2) Impact of having more ferries

Next, we investigate as to whether having more ferries helps to improve the detection faster and hence improves the delivery ratio even more. We tried using 1, 2 and 4 ferries. The ferry routes are as shown in Figure 1. The rest of the simulation parameters are the same as in the 1st set of experiments (i.e. 8 malicious nodes, each flow generates 1 pkt/s etc). Table 2 tabulates our results. In this table, we include the overall overhead which is measured as the ratio of the total number of transmitted bytes to the total number of received bytes. The extra overhead measures the additional overhead that need to be sent for the intrusion detection and mitigation scheme. The results in Table 2 indicate that the delivery ratio after mitigation improves with more ferries. Specifically, the delivery ratio after mitigation improves to 93.1% when there are four ferries. The extra overhead is very small compared to overall overhead.

# of ferries	1	2	4
Delivery ratio after mitigation	86.9%	90.2%	93.1%
Extra overhead for intrusion detection and mitigation	0.24	0.24	0.25
Overall overhead	10.51	11.42	12.04

Table 2: Performance of FBIDM with more ferries.

3) Impact of ferry speed

In our third set of experiments, we investigate the impact of ferry speed on the intrusion detection and mitigation performance. We use only one ferry but vary the ferry speed. Table 3 tabulates our results. Our results indicate that the delivery ratio improvement is better with faster ferry. However, the improvement is not as good as the case where more ferries are introduced.

Ferry Speed (m/s)	20	30	40
Delivery ratio after mitigation	86.9%	88.2%	89.8%
Extra overhead for intrusion detection and mitigation	0.24	0.24	0.24
Overall Transmission Efficiency	10.51	10.93	11.37

Table 3: Performance of FBIDM with different ferry speeds.

4) Impact of blackhole attacks

In our fourth set of experiments, we investigate the scenario where the malicious nodes drop all the data packets rather than only 50% of the data packets. We use 1 to 4 ferries, each ferry travels at 20 m/s. Without any mitigation scheme, the delivery ratio drops to 65.9% when 8 malicious nodes launch blackhole attacks. Our results with the FBIDM scheme are tabulated in Table 4. Our results show that the delivery ratio improvement degrades slightly (when compared to the selective dropping attack case). The achievable delivery ratio degrades from 86.9% (for selective dropping attacks) to 82.9% for the single ferry case and from 93.1% (for selective dropping attacks) to 91.9% in the 4 ferries case with blackhole attacks.

# of ferries	1	2	4
Delivery ratio after mitigation	82.9%	86.6%	91.9%
Extra overhead for intrusion detection and mitigation	0.26	0.27	0.27
Overall Transmission Efficiency	9.93	10.62	11.12

Table 4: Performance of the FBIDM scheme with 100% data dropping by malicious nodes.

5) Impact of combined rushing and data dropping attacks

Next, we investigate the impact of combined rushing and data dropping attacks. Recall that in the DSR routing scheme, normally the nodes backoff a random amount of time before relaying the route requests. With rushing attacks, malicious nodes immediately relay the route requests in the hope that they will be chosen as the intermediate nodes in the forwarding path. We use 50 nodes in a 2000x2000 m^2 for this experiment. Malicious nodes which launch the rushing attacks will drop 50% of the data packets if they are chosen to be intermediate forwarding nodes. Our results show that without mitigation, the delivery ratio drops to 73.5% with combined attacks and the FBIDM scheme improves the delivery ratio to 84.3% but the ENDORSE scheme only manages to improve the delivery ratio to 75.9%.

VI. CONCLUDING REMARKS AND FUTURE WORK

In this paper, we first describe an intrusion detection and mitigation scheme called the ENDORSE scheme that was designed for well connected adhoc networks. Intrusion detection chemes designed for well connected adhoc networks may not work well in sparsely connected networks. Thus, we present a new ferry-based intrusion detection and mitigation (FBIDM) scheme for sparsely connected adhoc networks. We then conduct simulation experiments to compare the two schemes in a sparsely connected adhoc network. Our results indicate the ineffectiveness of the ENDORSE scheme in a sparsely connected adhoc network. Our results also show that our FBIDM scheme can mitigate effectively against the data dropping attacks in sparsely connected adhoc network. This is just a preliminary work. We intend to study the performance of the FBIDM scheme in new attack scenarios e.g. malicious nodes not returning custody transfer acknowledgements. Last but not least, we intend to investigate the effectiveness of the FBIDM scheme in disruption tolerant networks (DTNs) that run different DTN routing schemes. Our results will be reported in a future journal paper.

REFERENCES

[1] C Perkins, etc, "Ad Hoc On-Demand Distance Vector (AODV) Routing", IETF internet draft, draft-ietif-manet-aodv-11.txt, 2002.

[2] D. B. Johnson, D. Maltz, "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, edited by T. Imielinski and H. Korth, Chapter 5, pp 153-181, Kluwer Academic Publishers, 1996.

[3] J. Hsu, et al, "Performance of Mobile Adhoc Networking Routing Protocols in Realistic Scenarios", Scalable Network Technologies White Paper, 2004.

[4] P. Papadimitratos, Z. Haas, "Secure routing protocol for mobile adhoc networks", SCS Communication Networks and Distributed System Modeling and Simulation Conference, Jan, 2002.

[5] Y.C. Hu etc, "Ariadne: A secure on-demand routing protocol for adhoc networks", 8th ACM International Conference on Mobicom, Sept, 2002.

[6] Y.C. Hu etc, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", Proceedings of IEEE 4th Workshop on Mobile Computing Systems and Applications, June 2002.

[7] C. Perkins, P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers", Proceedings of ACM Sigcomm, 1994.

[8] A. Perrig etc, "Efficient and secure source authentication for multicast", Network and Distributed System Security (NDSS) Syposium, Feb 2001.

[9] Y.C. Hu etc, "Packet leashes: a defense against wormhole attacks in wireless adhoc networks", Proceedings of the IEEE Infocom, April 2003.

[10] S. Marti etc, "Mitigating routing misbehavior in mobile adhoc networks", 6th ACM International Conference in Mobile Computing and Networking, Aug 2000.

[11] B.Awerbuch etc, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures", Proceedings of ACM WiSe, 2002.

[12] P. Papadimitrators, Z. Haas, "Secure data transmission in mobile adhoc networks", 2nd ACM Workshop on Wireless Security (WiSe), 2003.

[13] Y. Huang, W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", Proceedings of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.

[14] Y. Hu, A. Perrig, D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols", Proceedings of ACM WiSe, 2003.

[15] M. Chuah, P. Yang, B. Davison, L. Cheng, "Store-and-Forward Performance in a DTN", VTC poster, Proceedings of IEEE VTC, 2006.

[16] M. Chuah, P. Yang, "Energy Efficient Adhoc Networks with DoS Resilience", Lehigh CSE Technical Report, August, 2005. Also accepted 1st Network/Computer Security Workshop, Lehigh University, Aug, 2005.

[17] K. Fall, W. Hong, S. Madden, "Custody Transfer for Reliable Delivery in Delay Tolerant Networks", IRB-TR-33-030, July 2003.