A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs

Sureyya Mutlu
Computer Engineering Department
Turkish Air Force Academy
Istanbul, Turkey
s.mutlu@hho.edu.tr

Guray Yilmaz
Computer Engineering Department
Turkish Air Force Academy
Istanbul, Turkey
g.yilmaz@hho.edu.tr

***Abstract*— Mobile Ad Hoc Network (MANET) is a collection of nodes, which form an infastructureless topology. There is no central access point or centralized management. For their nature, MANETs present a number of unique problems for Intrusion Detection Systems (IDS). This paper introduces an intrusion detection framework for MANETs, which is based on trust relationship. In our proposed framework, intrusion detection system relies on local and global determination of attacks within network and carried out in a distributed fashion with cooperation among nodes. Trust in this manner is an important issue. The nodes watch suspicious activities of neighboring nodes. An intrusion detection alert message is disseminated throughout the network to report the anomaly. Reputation of intrusion detection alert messages is used for trust assessment. The proposed framework aims to utilize a distributed and cooperative trust based intrusion detection system to cope with the disadvantages drawn from mobility of nodes and the probability of selfishness, which are unique to MANETs.**

Keywords*— Mobile Ad Hoc Networks; Trust Management; Intrusion Detection Systems.

I. Introduction

Mobile Ad Hoc networks (MANETs) have received considerable attention in recent years. A mobile ad hoc network is a collection of autonomous nodes, which form an infastructureless topology. The network topology dynamically changes as nodes join and move out of the network. There is no central access point or centralized management. Routing and other network operations are carried out by individual nodes. Each node acts as a wireless router and routes packets to neighbor nodes to reach intended destination. Therefore, ad hoc networking has been proven to be a promising solution to increase the radio coverage of broadband wireless systems in an infastructureless fashion.

MANETs are ideally suited for applications where such infrastructure is either unavailable or unreliable. Typical applications include military communication networks in battlefields, emergency rescue operations and environmental monitoring [1].

The wireless characteristics of transmission medium imply limited bandwidth and high error rate in radio transmission. Thus, the key point in designing a protocol for MANETS is the effective use of bandwidth. On the other hand, mostly, MANETs are formed of battery-powered devices such as laptops, PDAs and so on in which power consumption is critically important. Moreover, the availability of an individual node cannot be assured and therefore, services cannot rely on a central entity and must be provided in a distributed and adaptive manner [2]. MANETs need well-organized distributed algorithms to determine network organization, link scheduling, and routing.

Because network topology can change at any point of time, conventional routing will not work in MANETs. Ad hoc routing protocols can be classified into two types; proactive and reactive. In proactive protocols nodes in a wireless ad hoc network keep track of routes to all possible destinations. The route is identified in advance. In case of a topology change, this modification needs to be disseminated throughout the entire network. On the other hand, reactive protocols will figure out the routes when required by the source node, as needed. When a node needs to send packets to several destinations but has no route information, it will start a route detection process within the network. Routing protocols in ad hoc networks need to deal with the mobility of nodes and constraints in power and bandwidth [3].

Due to their nature, MANETs are more vulnerable to security attacks than wired networks. Security in wireless ad hoc networks is principally difficult to maintain, particularly because of the limited physical protection of each individual node, the irregular characteristics of connectivity, the lack of certification authority, centralized monitoring or management. Unlike wired networks where an adversary must gain physical access to the network or pass through several lines of defense at firewalls and gateways, attacks on a wireless network can come from all directions and target at any node. That is why every node must be prepared for attacks directly or indirectly. Additionally, an attack from a compromised node within the network is far more damaging and much harder to detect [2].

MANETs are subject to passive and active attacks. The passive attacks typically involve only eavesdropping of data, whereas the active attacks involve actions performed by adversaries such as replication, modification and deletion of exchanged data. Specifically, attacks in MANET can cause congestion, propagate incorrect routing information, prevent services from working properly or shutdown them completely [4].

MANETs present a number of unique problems for Intrusion Detection Systems (IDS). Monitoring traffic by promiscuously within wireless radio range is a limiting factor in IDS on MANETS. Another problem is the mobility of the nodes. Additionally, a node in ad hoc network is more vulnerable to compromise. Also, because of the dynamic network topology of MANETs, an IDS may not be able to obtain enough sample data for accurate intrusion detection [5].

In this paper, we proposed a trust based distributed and collaborative intrusion detection framework for MANETs. Section 2 summarizes related work and proposed IDSs on MANETS relevant to our approach. Our proposed model is presented in Section 3, and finally, conclusion and future work are given in Section 4.

II. RELATED WORK

Because of their own characteristics, IDSs for traditional wired networks do not suit well for MANETs. There have been several proposals for Intrusion Detection Systems on MANETs [6-18].

One general approach for IDS on MANETs is distributed and cooperative architecture. In this architecture all nodes in MANET have their own local IDS system. Nodes come to a decision in a distributed fashion cooperatively. Upon determination of an intrusion, nodes share this information, asset attack risk degree and take necessary actions to eliminate the intrusion using active or passive precautions.

Other IDS architectures in MANETs are stand-alone and hierarchical IDSs. In stand-alone architectures every node performs IDSs locally without collaborating and respond locally. This IDS architecture has a drawback for network attacks. In hierarchical IDS architectures, MANETs are grouped into clusters or zones. One of the nodes in a zone/cluster is responsible for IDS. IDS is carried out in a distributed fashion and with collaboration with other clusters/zones. The main advantage of this architecture is effective use of constraint resources but has a drawback for highly mobile MANETs for establishing zones and detecting responsible nodes in clusters.

A. Distributed and Cooperative IDS

The first IDS for MANETs proposed by Zhang and Lee is a distributed and cooperative IDS [1][6]. In this architecture, each node detects intrusions locally and come to a decision globally if the local evidence for a network attack is inadequate. Respond may be local or global depending on the coordination among neighborhood nodes.

Statistical anomaly-based detection is preferred since rules cannot be updated in a wireless ad hoc environment over misuse base detection. The statistical anomaly-based detection composes the local data for IDS.

A multi-layer intrusion detection and response is proposed allowing different attacks at the most effective layer. It is believed to achieve a higher detection rate with a lower false positive rate.

Ad Hoc On-Demand Distance Vector [19] (AODV), Dynamic Source Routing [20] (DSR) and Destination-Sequenced Distance Vector [21] (DSDV) algorithms are used to have a better rate and false alarm rate metrics.

The system is reliable if the majority of the nodes are not compromised [1]. Additionally, the collaborative detection mechanism is susceptible to denial of service and spoofed intrusion attacks.

B. Zone Based Intrusion Detection System

Sun B et al. proposed a non-overlapping zone-based IDS [22]. In this architecture, the network is divided into zones based on geographic partitioning to save communication bandwidth while improving detection performance by obtaining data from many nodes. The nodes in a zone are called *intrazone nodes*, and the nodes which work as a bridge to other zones are called *interzone (gateway) nodes*. Each node in the zone is responsible for local detection and sending alerts to the interzone nodes. Their framework aims to allow the use of different detection techniques in each IDS agent.

Intrazone nodes carry out local collection and correlation, while gateway nodes are responsible for global collection and correlation to make final decisions and send alarms. Therefore, only gateway nodes participate in intrusion detection. The alerts sent by interzone nodes simply show an assessment of the probability of intrusion; the alarms generated by gateway nodes are based on the combined information received. In their aggregation algorithm, gateway nodes use the following similarities in the alerts to detect intrusions: classification similarity (classification of attacks), time similarity (time of attack happening and time of attack detection) and source similarity (attack sources). Source similarity is the main similarity used, so the detection performance of aggregation algorithm could decrease with increasing number of attackers.

The advantages of an aggregation algorithm using the data from both partial and full victims are emphasized: lower false positive and higher detection rate than local IDS achieves. Nevertheless, its performance can decrease with the existence of more than one attacker in the network. They also conclude that communication overhead is increased in proportion to mobility where local IDSs generate more false positives and send more intrusion alerts to gateway nodes. In addition, aggregating data and alerts at interzone nodes can result in detection and response latency, when there is sufficient data for intrusion detection even at intrazone nodes.

C. General Cooperative Intrusion Detection Architecture

A cooperative and dynamic hierarchical IDS architecture, which uses multiple-layering clustering, is proposed by Sterne et al. in [23]. At the beginning, the nodes are assigned to clusters and first level clusters act as a management focus for IDS activity of immediate surrounding nodes. Then, these first level clusters form a second layer clusters. This process goes on until all nodes are assigned to a cluster. To avoid single point of failure, they propose choosing more than one cluster-head for the top-level cluster. The selection of cluster heads is based on topology and other criteria including connectivity, proximity, resistance to compromise, and accessibility by network security specialists, processing power, storage capacity, energy remaining, bandwidth capabilities and administratively designated properties.

In this dynamic hierarchy, data flow is upward, while the command flow is downward. Data are acquired at leaf nodes and aggregated, reduced and analyzed as it flows upward. The key idea is given as detecting intrusions and correlating with other nodes at the lowest levels for reducing detection latency and supporting data reduction, even as maintaining data sufficiency. It supports both direct reporting by participants and promiscuous monitoring for correlation purposes.

This architecture targets military applications with high scalability and reduced communication overhead through hierarchical architecture [23]. However, the cost of configuration of the architecture in dynamic networks should also be considered.

D. *Intrusion Detection Using Multiple Sensors*

Kachirski and Guha propose an IDS solution based on mobile agent technology [24], which reduces network load by moving computation to data. This is a significant feature for MANETs that have lower bandwidth than wired networks.

Proposed IDS structure distributes the functional tasks by using three mobile agent classes: monitoring, decision-making and action-taking. The advantages of this structure are given as increased fault tolerance, communication cost reduction, improved performance of the entire network and scalability.

Hierarchically distributed IDS architecture divides the network into clusters. Cluster-heads are selected by voting for a node, which is based on its connectivity. Each node in the network is responsible for local detection. Only cluster-heads are responsible for detection using network-level data and for making decisions. Cluster nodes can respond to the intrusions directly if they have strong evidence locally. If the evidence is insufficient, they leave decision-making to cluster heads by sending anomaly reports to them.

In this proposal although, a scalable and bandwidth-efficient IDS is proposed by using mobile agents, but security issues for mobile agents are need to be investigated.

E. *DEMEM: Distributed Evidence Driven Message exchanging ID Model*

DEMEM [25] is a distributed and cooperative IDS in which each node is monitored by one-hop neighbor nodes. In addition to one-hop neighbor monitors, 2-hop neighbors can exchange data using intrusion detection (ID) messages. The main contribution of DEMEM is to introduce these ID messages to help detection, which they term evidence-driven message exchange.

Evidence is defined as the critical information (specific to a routing protocol) used to validate the correctness of the routing protocol messages, for instance, hop count and node sequence number in AODV. To minimize ID message overhead ID messages are sent only when there is new evidence, (it is called evidence-driven). DEMEM also introduces an ID layer to process these ID messages and detect intrusions between the IP layer and the routing layer without modifying the routing protocol, so it can be applied to all routing protocols.

DEMEM uses the specification-based IDS model. There are nodes called Multipoint Relays (MPRs), which serve to reduce the flooding of broadcast packets in the network. These nodes are selected by their neighboring nodes called MPR selectors. The packets of an MPR node's MPR selectors are only retransmitted by that MPR node. Topology control messages are sent by each node periodically to declare its MPR selectors.

DEMEM cannot detect collaborative attacks. For example, two attackers who falsely claim that they are neighbors might not be detected by the above constraints.

DEMEM introduces three authenticated ID messages for Optimized Link State Routing Protocol [20] (OLSR).

- The first message is ID-Evidence, which is designed for two-hop-distant detectors to exchange their evidence concerning one-hop neighbors, MPRs and MPR selectors on OLSR.
- The second message, ID-Forward, is a request to forward any held ID-Evidence messages to other nodes. This means that a node can request the holder of evidence to forward it directly, rather than sending it itself, so reducing message overhead.
- The last message, ID-Request, is designed to tolerate message loss of ID-Evidence with low communication overhead. The false positives and delay detection due to message loss are decreased by an ID-Request message. Moreover, they specify a threshold value to decrease false positives due to temporary inconsistencies resulting from mobility. When a detector detects an intrusion, it automatically seeks to correct the falsified data.

III. DICOTIDS: DISTRIBUTED COOPERATIVE TRUST BASED INTRUSION DETECTION ARCHITECTURE FOR MANETs

In this section, we propose a distributed cooperative trust based intrusion detection architecture for MANETs. The architecture is based on running Local Intrusion Detection engines in each node independently. The objective is to monitor all network activity within wireless range to detect misbehaving nodes on promiscuous mode. That means, if node A is in wireless range of node B, it can watch communication activity to and from B even node A is not involved in. Accruing intrusion detection data in this manner has significant advantage. First, it allows local data collection without consuming any additional communication overhead. Second, it provides first hand observations, which means no need to rely on observations from other nodes, which might be false.

Moreover, intrusion detection is distributed throughout the network in case of weak or inconclusive evidence of anomaly. A global investigation is initiated to support local intrusion detection.

Flooding algorithm is used to share IDS alert messages. Flooding is the mechanism by which a node receives a flooded message for the first time, it rebroadcasts that message once. Each node is responsible to deliver the message to its neighbor within wireless transmission range.

DICOTIDS mainly focus on detecting compromised modes in network. A compromised node can disseminate false IDS alert messages or drop the IDS alert message flooded by other nodes. Therefore, a trust mechanism is established in the network. Trust management can mitigate nodes' selfish behaviors', such as dropping messages or unwillingness for cooperation. Reputation mechanism is used as a dynamic rating system.

Once, a node detects misbehavior of a neighbor node or suspicious activity, it starts a distributed IDS algorithm by broadcasting IDS alert messages. Nodes periodically share their respective data by flooding algorithm and then start a diagnostic phase. After the diagnostic phase in which all collected data from other nodes are compared, trust evaluation phase starts. If a trustworthy node broadcast an IDS alert message, intrusion response is activated even if the relevant node is not directly involved in IDS assessment. Trust management is maintained by watching the neighbor nodes activities whether they rebroadcast the IDS alert messages or not. A reputation mechanism is used to evaluate the trust level of a node. Figure 1 depicts the components of the framework.

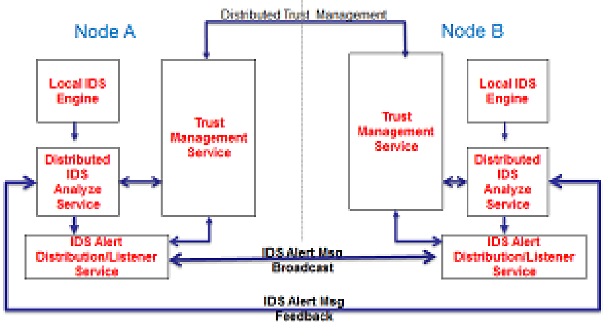
Distributed Trust Management
Node A
Node B
Local IDS Engine
Trust Management Service
Distributed IDS Analyze Service
IDS Alert Distribution/Listener Service
IDS Alert Msg Broadcast
Trust Management Service
Local IDS Engine
Distributed IDS Analyze Service
IDS Alert Distribution/Listener Service
IDS Alert Msg Feedback

Figure 1. Components of DICOTIDS

The details of the framework are described as follows:

A. *Local IDS Engine:*

The first phase of the intrusion detection process starts at Local Intrusion Detection engine. It sniffs the neighbor nodes network activity in promiscuous mode. The engine runs a popular network-based IDS, which is the open-source Snort [26]. Snort is able to sniff the network activity in promiscuous mode and configured with a rule set it can function as a real-time IDS. A Snort rule set is a file of attack signatures. A match to a signature means that an attack is recognized. Each node assumed to have the database of these rule sets and functions as a real-time detection system.

Once an intrusion attempt or a suspicious activity is determined, all relevant data is passed to distributed IDS analyze service.

B. *Distributed IDS Analyze Service:*

IDS analyze service will use outputs of the Local IDS engine as well as IDS alert messages disseminated from other nodes. If there is enough evidence for intrusion, this service will put intrusion prevention measures into effect and forward the related information to IDS alert distribution service to inform the other nodes in the network. If there is weak or inconclusive evidence of anomaly IDS analyze service will request global analysis. Only the replies from the trusted nodes will be taken into consideration.

The functional diagram of Distributed Analyze Service is depicted in Figure 2. The service will also try to verify the attack by additional IDS Alert messages originated from other nodes in the network.

If the evidence comes via IDS alert message from another node in the network, first the trust level of the sender node is checked and;

- If the message is from a trusted node and there is more than one trusted node disseminating IDS alert message, than there is strong evidence for an intrusion attempt.
- If the IDS alert message is from an untrustworthy node, the IDS message is ignored.
- If the message is from a node, which the trust level has not been evaluated yet, then special interest is performed.
- If the intrusion alert is supported more than a single (trust level undecided) node or an intrusion is also approved by local IDS, the service may conclude of an intrusion.

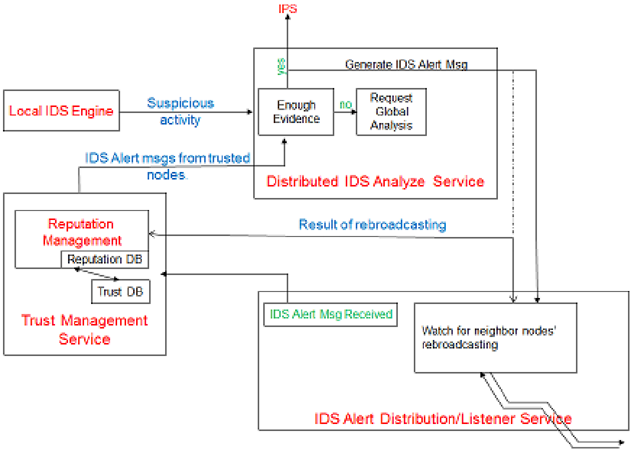

Figure 2. Functional Diagram of Distributed Analyze Service

Once the service concludes for an intrusion, first it will inform the Intrusion prevention module to take necessary actions in order to prevent intrusion. The next is to pass this information to IDS alert distribution service. The information

ISBN: 978-1-61208-133-5

includes nodes involved in the intrusion attempt, type of attack, priority, strength, timestamp etc.

The last thing is to inform the trust management service to downgrade or set the trust level of the involving node to untrustworthy.

C. IDS Alert Listener / Distribution Service:

This service is responsible to broadcast the IDS alert messages within wireless radio range and watches for the neighbor nodes if they rebroadcast the message within a time frame. Each message will have a unique message number and detected intrusion related information. IDS alert message contains:

- Originator ID and Originator Message ID (null if produces for the first time)
- Sender Node ID
- Sender Message ID
- Compromised/Attacker node's ID/IP
- Attack Type
- Classification
- Priority
- Date/time

Immediately after, this service will inform the trust management service to evaluate reputation values. If the neighbor nodes rebroadcast the IDS alert message without any modification, trust management service will perform the reputation update procedures accordingly. In addition, if this does not occur in a limited time frame or the rebroadcasted IDS alert message is corrupted then reputation and trust assessment is evaluated as described below.

IDS listener service sniffs the neighbor node's activities in promiscuous mode for the rebroadcasted messages. Upon receipt of an IDS alert message, the message is passed to distributed IDS analyzer and trust management service.

D. Trust Management Service:

Trust management service is responsible to maintain relationships among nodes in the network. This service will mitigate misbehaving of nodes and enforce cooperation. Projected trust management is derived form a reputation based scheme proposed by Jiangy hu [27]. Figure 3 depicts the components of the service.

Trust in a node is associated with its reputation value. There are three trust levels and we use a trust value T, to represent the trustworthiness of a node. A node considers another node B either

- Trustworthy, with T = 1,
- Untrustworthy, with T = -1, or
- Trustworthy undecided, with T = 0

A trustworthy node is a well-behaved node that can be trusted. An untrustworthy node is a misbehaved node and should be avoided in distributed IDS evaluation process. A node with undecided trustworthiness is usually a new node in the network and special interest should be taken in IDS evaluation process.

Each node keeps a reputation table, which associates a reputation value with each of its neighbors. It updates the table on direct observation only. Reputation value of a neighbor node will not be distributed globally and will be stored locally. Reputation values will be shared only if requested by other nodes.

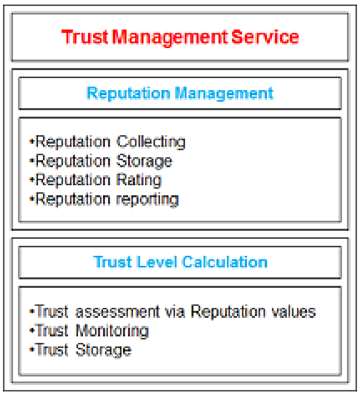

Figure 3. Components of Trust management Service

Reputation values R are between a range of $0 \leq R \leq 1$ and there is one threshold R_t,

$R \geq R_t$ for trustworthy and

$R < R_t$ for untrustworthy.

For a new node N with reputation value R and trust value T,

- $T = 1$, if $R \geq R_t$
- $T = -1$, if $R < R_t$
- $T = 0$, if $R < 0$

Reputation values depend on the behaviors of the node. If a node broadcasts an IDS alert message, then it sniffs the neighbor nodes in promiscuous mode. If that node rebroadcasts the IDS alert message, the originator node promotes the reputation value for that node; otherwise, the reputation value is downgraded. If the rebroadcasted message is modified the nodes trust value will be in untrustworthy state. *R* is the proportion of the total number of forwarded messages to the total number of sent messages.

Each node keeps track of the neighbor nodes and establishes reputation values directly. If a node needs to query a specific node that is beyond the wireless radio range, it will ask for reputation values to all the trusted nodes in the network. The average of the replies will set the reputation value for the requested node.

Another factor for a node that will affect it is trust level is the correctness of the IDS alert message. All the nodes that receive an IDS alert message will also monitor the evidences. If there is not enough evidence, the IDS message is concluded to be false. So that the trust level for the disseminating false messages node will be untrustworthy.

E. Pseudo Code for DICOTIDS :

- ***Local IDS Engine (LIDS)***

```
Watch for Neighboring Node's Network Traffic
Compare Net Traffic with IDS Signature Database
If Network Activity Matches IDS Signature
    Create IDS Alert Msg
    Pass IDS Alert Msg to Dist. IDS Analyze Service
```

ISBN: 978-1-61208-133-5

```
     Inform Trust Management Service
   Endif
```

- ***Distributed IDS Analyze Service***

```
   For each IDS Alert Msg received form LIDS do
   If there is strong evidence
      Activate IPS
      Forward IDS Alert Msg to Distribution Service
      Inform Trust Management
   Else
      Request Global Analyze
   Endif
 For each IDS Alert Msg received from the network
    Check Trust Level of the sender
    If the sender is a trusted node
      Activate IPS
      Forward IDS Alert Msg to Distribution Service
     Else
      Ignore message
      Inform Trust Management
    Endif
    If the sender's trust level is not assigned
      If there is more than one sender
        Activate IPS
        Forward IDS Alert Msg to Distribution Service
        Inform trust Management
        Request Global Analyze for confirmation
      Else
      Request Global Analyze
 Endif
```

- ***Distribution/Listener Service***

```
    Broadcast IDS Alert Message
    Listen for the neighboring nodes to rebroadcast
    Inform Trust Service for successful rebroadcasts
    Inform Trust Service for unsuccessful rebroadcasts
```

- ***Trust Management Service***

```
    Evaluate the reputation value for each neig nodes
    For each neighboring node
       If reputation value is greater than the threshold
           Assign node's Trust Level as Trustworthy
       Else
           Assign node's Trust Level as Untrustworthy
       Endif
    Update databases respectively
```

IV. SIMULATION AND PEFFORMANCE ANAYSIS

The objective of simulation and performance analysis is to determine the feasibility of DICOTIDS in MANETs where there are a number of malicious nodes. The metrics to evaluate the performance are described below.

A. Metrics

IDS Alert Message Delivery Ratio: The ratio of the IDS alert message delivered to the destination nodes. The delivery ratio is directly affected by uncooperative behavior, number of malicious nodes, and packet loss.

Message Overhead: The ratio of redundant messages to the total number of messages relevant to the IDS instance.

The number of IDS instances to evaluate the trust level of nodes: The reputation rates are directly involved in evaluating the trust level of a node in coherence with the reputation threshold value.

B. Simulation and Results

We have partially simulated the DICOTIDS in Network Simulator (NS-2) [28]. For all the metrics we want to evaluate, we used fixed parameters for network environment. Also, we assumed that every node has a Local Intrusion Detection System (LIDS) with updated signatures.

We ran the simulation for two scenarios.

Scenario #1: Few ($n<3$) malicious nodes with a total number of 15 nodes.

Scenario #2: More ($n>7$) malicious nodes with a total number of 15 nodes.

C. Analysis

As the number of malicious nodes in the network increase, the IDS alert delivery ratio is decreased proportionally. The layout and the mobility of the nodes have an impact in the ratio also. However, mostly this ratio satisfied the requirements of the whole system.

In some cases, especially with a high dense node layout, several nodes initiated the distributed IDS analysis process for the same instance. Because the reputation values and trust levels are stored and evaluated locally, the disharmony among nodes resulted in the increase of redundant message. However, this did not have a crucial effect on the total performance.

In order to determine untrusted nodes and successfully identify malicious nodes, a number of intrusion instances are required. On the first occasion of an intrusion attempt, nodes need to rely on local intrusion detection system (LIDS). But, as the number of instances increase, accurate reputation values and trust levels are evaluated respectively.

Additionally, the reputation threshold value (R_T) should be set to lower values for fixed or low mobile networks rather than the value for highly mobile networks.

The proposed framework should be feasible for networks with nodes with low mobility. On the other hand, we assumed that all nodes have the same emitting power. That means with different emitting powers, reputation mechanism may fail for the event that node B is in the range of node A, but node A is not in the range of node B.

V. CONCLUSION

A trust based distributed intrusion detection framework is proposed in order to protect nodes from performing misbehavior or selfish behavior in MANETS. Trust, in the framework, is mainly based on direct observation, but indirect observations are also applied. The proposed infrastructure provides robustness against the propagation of false trust information by malicious nodes.

A dynamic and collaborative ad hoc intrusion detection system has been proposed. Our approach does not modify or restrict the network discovery or routing protocols. The concepts discussed in this paper are in broad sense that they can easily be integrated to existing routing protocols.

We aim to fully simulate the framework in NS-2 [28], an open source network simulator. The message overhead and resistance to intrusion in relevant to the number of compromised nodes in the network is critical. In addition, the effects of the mobility of the nodes in the network need to be observed. Additionally, testing the model using different routing protocols will conclude valuable data.

REFERENCES

[1] Y Zhang and W.Lee, Intrusion Detection In Wireless Ad Hoc Networks. In proc of the 6th Int Conf on Mobil Comput and Netw (MOBICOM), 2000, pp. 275-283

[2] S. Sen and J.A.Clark, Intrusion Detection in Mobile Ad Hoc Networks, Guide to Wireless Ad Hoc Networks, Computer Communications and Networks, 2009, pp. 441-442

[3] K. Pathan and C.S. Hong, Routing in Mobile Ad Hoc Networks, Guide to Wireless Ad Hoc Networks, Computer Communications and Networks, 2009, pp.63-66.

[4] L. Zhou and Z. Haas, Securing Ad Hoc Networks, IEEE Network Magazine, vol. 13, no. 6, 1999. pp.21

[5] P. Brutch and C. Ko, Challenges in Intrusion Detection for Ad Hoc Networks, IEEE Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.

[6] Y. Zhang and W. Lee, Y-A. Huang, Intrusion detection techniques for mobile wireless networks, Wireless Networks, vol. 9, 2003, pp. 545-556.

[7] R. Ramanujan, A. Ahamad, J. Bonney, R. Hagelstrom, and K. Thurber, Techniques for intrusion-resistant ad hoc routing algorithms (TIARA), IEEE MILCOM 2000, Los Angeles, 2000, pp. 660-664.

[8] S. Buchegger and J-Y. Le Boudec, Performance analysis of the CONFIDANT protocol (Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks), 3rd ACM Int. Symp. on Mobile Ad Hoc Networks and Computing, Switzerland, 2002, pp. 226-236.

[9] M. Kuchaki Rafsanjani, A. Movaghar, and Faroukh Koroupi, Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes, World Academy of Science, Engineering and Technology 44, 2008, pp.351-355.

[10] R. Puttini, J-M. Percher, L. Me, and R. de Sousa, A fully distributed IDS for MANET, 9th Int. Symp. on Computers and Commun. (ISCC 2004), 2004, pp. 331-338.

[11] G. Vigna, et al., An intrustion detection tool for AODV-based ad hoc wireless networks, Annual Computer Security Applications Conf. (ACSAC 2004), Tuscon, 2004, pp. 16-27.

[12] A. Pirzada and C. McDonald, Establishing trust in pure ad-hoc networks, 27th Australian Conf. on Computer Science, Dunedin, New Zealand, 2004, pp. 47-54.

[13] Y. Rebahi, V. Mujica, and D. Sisalem, A reputation-based trust mechanism for ad hoc networks, 10th IEEE Symp. on Computers and Communications (ISCC 2005), 2005, pp. 37-42.

[14] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos, Detecting critical nodes for MANET intrusion detection, 2nd Int. Workshop on Security, Privacy, and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006), 2006, pp. 7-15.

[15] H. Yang, J. Shu, X. Meng, and S. Lu, SCAN: self-organized network-layer security in mobile ad hoc networks, IEEE J. on Sel. Areas in Communications, vol. 24, 2006, pp. 261-273.

[16] T. Chen and V. Venkataramanan, Dempster-Shafer theory for intrusion detection in ad hoc networks, IEEE Internet Computing, vol. 9, 2005, pp. 35-41.

[17] D. Subhadrabandhu, S. Sarkar, and F. Anjum, A framework for misuse detection in ad hoc networks - part II, IEEE J. on Sel. Areas in Communications, vol. 24, 2006, pp. 290-304.

[18] Y. Zhang and W.Lee, Intrusion Detection Techniques for Mobile Wireless Networks, Wireless Networks 9(5), 2003, pp. 545-556.

[19] C. E. Perkins, E. M. Royer, and S. R. Das, Ad hoc on-demand distance vector (AODV) routing. July 2000.

[20] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L.Viennot, Optimized link state routing protocol for ad hoc networks, in: IEEE International Multi Topic Conference, 2001, pp. 62–68.

[21] C. Perkins and P. Bhagvat, Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM Computer Communications Review, 1994, pp. 234-244.

[22] Sun B and Wu K et al. Zone-Based Intrusion Detection System for Mobile Ad Hoc Networks. Int J of Ad Hoc and Sens wireless Networks 2:3,2006

[23] D. Sterne and R. Balasubramanyam et al. A general Cooperative Intrusion Detection Architecture for MANETs. In Proc of the 3rd IEEE IWIA, 2005, pp.57-70

[24] O. Karchirski and R. Guha, Effective Intrusion Dtection Using Multiple Sensors in Wireless Ad Hoc Networks. In proc of the 36th IEEE Int Conf on Syst Sci (HICSS), 2003, pp.244-248

[25] C. Tseng and S.Wang, DEDEM: Distributed Evidence Driven Message Exchange Intrusion Detection Model for MANET. In proc of the 9th Int Symp on Recent Adv in Intrusion Detect LNCS 4219, 2006, pp.249-271

[26] Snort, <www.snort.org> 10.04.2011

[27] J. Hu and M. Burmester, Cooperation in Mobile Ad Hoc Networks, Guide to Wireless Ad Hoc Networks, 2009, pp.43-53.

[28] NS2, Network Simulator – 2, <www.isi.edu/nsnam/ns> 10.04.2011