JOURNAL OF AERONAUTICS AND SPACE TECHNOLOGIES
JULY 2013 VOLUME 6 NUMBER 2 (49-57)

SIMULATION AND PERFORMANCE ANALYSIS OF DISTRIBUTED COOPERATIVE TRUST BASED INTRUSION DETECTION FRAMEWORK FOR MANETs

Süreyya MUTLU
Turkish Air Force Academy
ASTIN, Computer Engineering Dept.
Yeşilyurt-İSTANBUL
s.mutlu@hho.edu.tr

Güray YILMAZ*
Turkish Air Force Academy
Computer Engineering Department
Yeşilyurt-İSTANBUL
g.yilmaz@hho.edu.tr

Received: *03rd April 2013,* ***Accepted:*** *03rd July 2013*

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. Intrusion detection in MANETs, however, is challenging for a number of reasons. This paper introduces intrusion detection architecture for MANETs, based on trust relationship and cooperation. In our proposed framework, intrusion detection system relies on local and global determination of attacks within network and intrusion detection is carried out in a distributed fashion. Reputation mechanism is used for trust assessment, which is obtained by watching the neighbor nodes behaviors. IDS alert messages are used to disseminate evidences of an intrusion attempt. A distributed IDS engine is the focal point of the architecture and we aim to utilize a cooperative trust based intrusion detection system to cope with the disadvantages drawn from mobility of nodes. In this paper, we present the feasibility of the proposed architecture by a detailed performance analyses according to the results obtained from simulations.

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

HAREKETLİ GEÇİCİ AĞLAR İÇİN DAĞITILMIŞ KOOPERATİF GÜVEN TABANLI SIZMA TESPİT SİSTEMİNİN SİMÜLASYON VE PERFORMANS ANALİZİ

ÖZET
Hareketli Geçici Ağlar (HGA) altyapısız bir topoloji oluşturan düğümler topluluğudur. Bu ağlarda, merkezi bir erişim noktası ya da merkezi bir yönetim söz konusu değildir. Bu özelliklerinden dolayı Saldırı Tespit Sistemi (STS) söz konusu olduğunda HGA'lar kendine özgü bir takım problemler ortaya koyarlar. Bu çalışmada HGA'lar için güven esasına dayalı bir saldırı tespit sistemi mimarisi ortaya konulmaktadır. Önerilen mimaride, saldırı tespit sistemi, saldırıların yerel ya da global tespitine ve düğümler arasındaki iş birliği ve güven esasına dayanmakta olup dağıtık olarak gerçekleştirilmektedir. Bu anlamda "güven" önemli bir sorun sahası oluşturmaktadır. Önerilen mimaride, düğümler, komşu düğümlerin muhtemel şüpheli davranışlarını izlemektedirler. Bir anomali söz konusu olduğunda ağ üzerinde STS uyarı mesajı yayınlanmaktadır. STS uyarı mesajlarının tekrarlanmasının izlenmesi sayesinde güven değerlendirilmesi yapılmaktadır. Önerilen mimari, iş birliği ile güven esasına dayalı, dağıtılmış bir STS ortaya koyarak, HGA'da düğümlerin devingenliğinden ve düğümlerin bencil davranma ihtimalinden kaynaklanan dezavantajları ortadan kaldırmayı hedeflemektedir.

Anahtar Kelimeler : *Hareketli Geçici Ağlar; Güven Yönetimi; Sızma Tespit Sistemleri.*

1. 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.

* Corresponding Author

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].

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 MANETs. Additionally, an attack from a compromised node within the network is far more damaging and much harder to detect [2].
Intrusion detection in MANETs, however, is challenging for a number of reasons [3, 4]. These networks change their topologies dynamically due to node mobility; lack concentration points where traffic can be analyzed for intrusions; utilize self-configuring multi-party infrastructure protocols that are susceptible to malicious manipulation; and rely on wireless communication channels that provide limited bandwidth and are subject to noise and intermittent connectivity [5].

Because of their own characteristics, Intrusion Detection Systems (IDSs) for traditional wired networks do not suit well for MANETs. There have been several proposals for Intrusion Detection Systems on MANETs [6-13].

One general approach for IDS on MANETs is distributed and cooperative architecture. In this architecture, all nodes in a 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, agree on 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.

The motivation behind this work is to establish a trust based Intrusion Detection architecture for MANETs and present the feasibility with simulation results. A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs (DICOTIDS) [14] mainly focus on detecting compromised modes in network in a dynamic fashion. MANETs need a distributed trust mechanism to identify compromised nodes in the IDS process. The paper mainly focuses on;

- Establishing a distributed relationship among nodes,
- Dynamically designating a reputation value for nodes in the network with direct observations,
- Establishing the trust levels cooperatively in a distributed manner,
- Finally, identifying compromised nodes with a distributed algorithm and sharing this information in the network.

The simulations and obtained results showed that, the proposed architecture should be feasible for networks like sensor networks, vehicular networks and networks where individual security is more important rather than military networks, which require error free, and precise security establishment.

In line with the proposed architecture and obtained results, the research shows that, Intrusion Detection in MANETS

- Require a dynamic and distributed algorithm to identify compromised nodes in a network,
- Collaboration and cooperation is a must but, subjective reputation values result in misidentification of compromised, and
- Distributed cooperative trust based intrusion detection mechanism suits well for public networks those do not require precise security considerations.

In this paper, we present a detailed performance analysis and feasibility of our proposed architecture DICOTIDS [14] with simulation results. Section 2 covers an overview of proposed architecture, Section 3 details the simulation and a detailed performance analysis and feasibility is presented at section 4. Finally, Section 5 concludes the paper.

2. BACKGROUND

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 if node A is not involved. Accruing intrusion detection data in this manner has significant advantages. 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 will start. If a trustworthy node broadcasts an IDS alert message, intrusion response will be 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. Fig. 1 depicts the components of the framework.

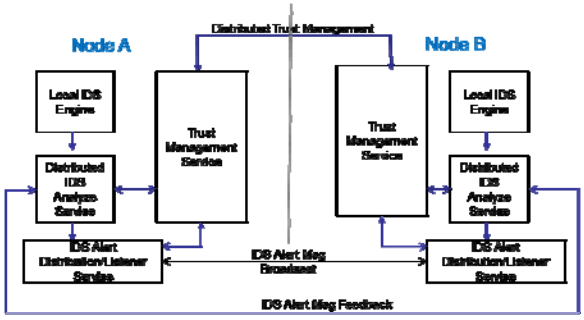

Fig. 1. Components of DICOTIDS.

The details of the framework are described as follows:

2.1 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 [15]. 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.

2.2 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 Fig. 2. The service will also try to verify the attack by additional IDS Alert messages originated from other nodes in the network.

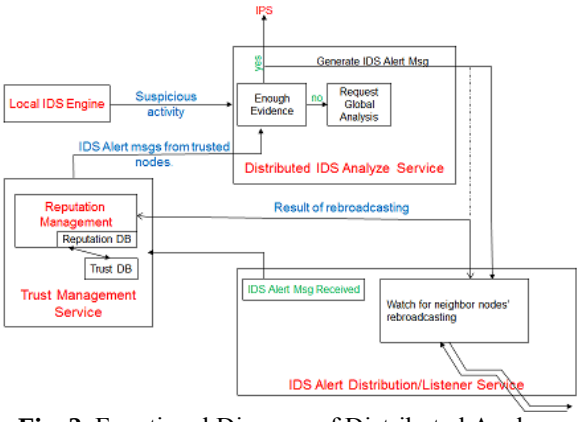

Fig. 2. Functional Diagram of Distributed Analyze Service.

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 alert 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 alert message is from an untrustworthy node, the IDS message is ignored.

- If the alert message is from a node, which the trust level has not been evaluated yet, then special interest is performed.
- If the alert message 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.

Once the service concludes for an intrusion, first it will inform the Intrusion prevention module to take necessary actions in order to prevent the intrusion. The next is to pass this information to IDS alert distribution service. The information includes nodes involved in the intrusion attempt, type of attack, priority, strength, timestamp, etc.

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

2.3 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 period. 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 period 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, this alert message is passed to the distributed IDS analyzer and the trust management service.

2.4 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 from a reputation based scheme proposed by Jiangy hu [16].

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.

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 its 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.

3. SIMULATION

In order to test the feasibility and performance analysis of the proposed architecture we have coded an event-driven simulation program. The simulation uses object-oriented structure and the *node class* encapsulates all the required properties relevant to the proposed architecture. Aim of the simulation is to provide a test bed for the basic properties of proposed intrusion system on MANETs.

3.1 Simulation Architecture

The simulation is designed to run in a two dimensional domain and carry out the basic functions of mobile ad hoc networks. Mobility and packet transfer are supported by the animated objects. Ontology is built up in accordance with the requirements of communication and the behaviors of nodes.

The events and communications between nodes are recorded to a log file and analyses data specific to the proposed architecture are presented to the user. Simulation is formed by an event list at design time. A snapshot of the simulation is presented in Fig. 3.

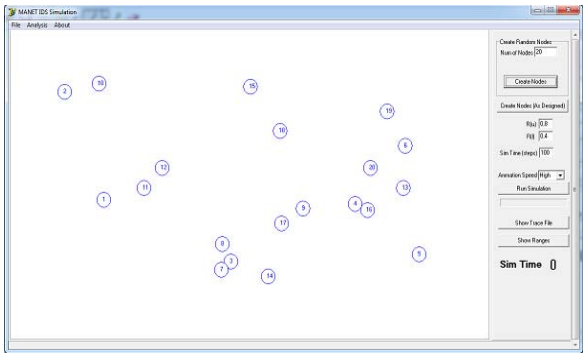

Fig. 3. Simulation snapshot.

3.2 Routing and flooding Algorithm

Simulation runs a reactive routing algorithm based graph theory and uses *Dijsktra* algorithm to establish the shortest path with minimum hops. Basic flooding algorithm is used for the broadcast requirements. Point to point communication is carried out by a packet frame consists of a header and a data frame.

3.3 Network Layout and Mobility

The network layout and mobility are designed in a dynamic fashion to accomplish different scenarios. It is possible to add various numbers of nodes to network with random mobility and random radio range coverage with upper and lower limits specified in advance. The aim to use different wireless range is to test the behaviors of nodes in which Node A is in the range of Node B while Node B is not in the range of Node A. In this manner, we aim to utilize a network with different network characteristics.

3.4 Scenarios

The simulation enables different scenarios with various numbers of nodes and with several intrusion techniques. Scenarios are combination of desired behaviors of nodes to be run at specific times. For example, 'Node 3 is to generate an *Intrusion Attempt* message at time 12'. Furthermore, basic network functions such as Ping and Reply Ping are utilized in simulation.

3.5 Simulation Algorithm

Simulation algorithm for the components of the proposed architecture is specified below.

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
  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

4. PERFORMANCE ANALYSES AND FEASIBILITY

We have simulated the DICOTIDS architecture performance analysis and feasibility with different network parameters to identify malicious nodes in network and observe the effects of threshold values used at the distributed intrusion analyze service, assessment of trustworthiness and distribution of reputation values and trust level information.

4.1 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.

The ratio of accurate trust level assessment: The ratio of accurate trust level assessment to the number of nodes in the network.

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.

4.2 Simulation and Results

We have run four scenarios (listed below) with different network parameters shown in Table-1.

Scenario 1: Medium dense layout without mobility
Scenario 2*:* Medium dense layout with low mobility
Scenario 3: High dense layout with low mobility
Scenario 4: High dense layout with high mobility

Table 1. Simulation parameters for scenarios.

Scenario	#1	#2	#3	#4
Number of nodes	20	20	30	30
Number of malicious nodes	1	1	3	3
Sim Time	100	100	100	100
Area (m.)	800x1000	800x1000	800x1000	800x1000
Wireless range	80-160	80-160	80-160	80-160
Mobility	Static	Dynamic	Dynamic	Dynamic

A number of simulations with one malicious node intruding neighboring nodes at a medium dense layout and without mobility network environment are carried out. 0.2 and 0.8 lower and upper threshold values are used accordingly.

The distributed intrusion analyses services at neighbor nodes to malicious node initiated the distributed IDS algorithm due to lack of enough evidence. Although most of them had identified the malicious node, significant number of the nodes could not evaluate the trust level of malicious node accurately. The average numbers of false positives are shown in Fig. 4.

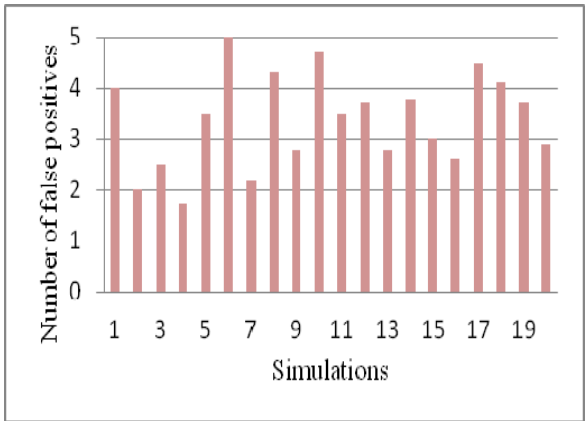

Fig. 4. Average number of false positives in simulations.

The simulations resulted in less false positives depicted at Fig. 5 with the same network parameters but having threshold values 0.4 and 0.8.

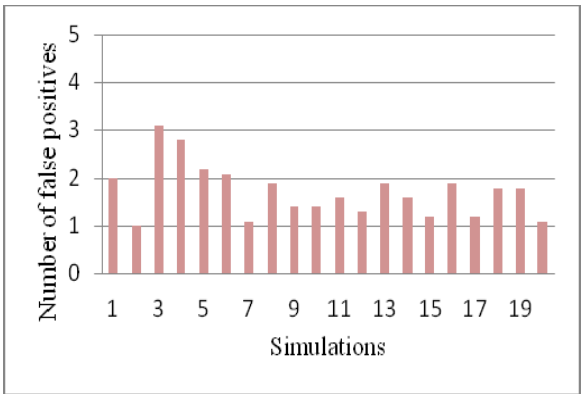

Fig. 5. Average number of false positives in simulations with revised threshold values.

To minimize the average number of false positives and assign accurate threshold values a series of simulations were carried out. It is observed that lower threshold value, ranging 0.38 to 0.42, minimizes the number of false positives. On the other hand, upper threshold value having 0.8 is monitored as the most stable value. It is assessed that the upper threshold value is a user choice. Using higher values result in more accurate assessments in assigning trust levels of nodes to *Trustworthy,* but an increase in the number of nodes with *trust level had not been evaluated yet* in the network. The relationship between the lower threshold value and the possibility of correct assessment is shown in Fig. 6.

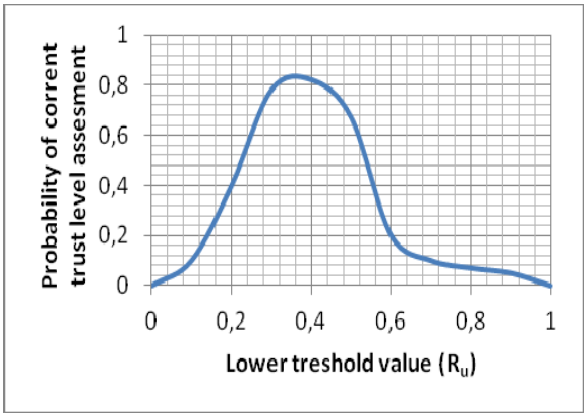

Fig. 6. Relationship between the lower threshold value and the probability of correct assessment.

It is also observed that the effects of mobility of the proposed architecture are limited. If the malicious node exists close to the center of the network, reputation values so the trust levels are evaluated more accurately than being at the edge of the network. Moreover, the overall performance is in direct relation with the number of intrusion instances originating from the same malicious node. As shown in Fig. 7, the average number of miss trust level assessments decrease as the number of intrusion instances increase.

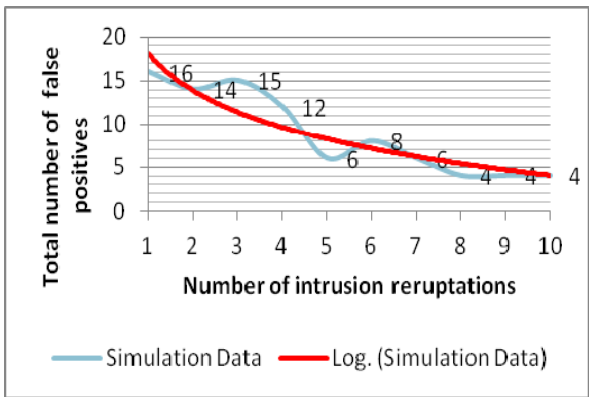

Fig. 7. Relationship of miss detection to the number of intrusion instances.

4.3 Analysis

We have simulated the proposed architecture with several scenarios and got different results for each of them.

First, we investigate the effects of mobility of the architecture. The results showed that there is a direct relationship among the mobility and layout, and system performance, but in all cases, the results satisfied the requirements of the system. The overall performance of the proposed architecture is more stable and the error rates are decreased if the malicious node is located at the center of the network rather than the edge. This is an expected result because the reputation values and the trust levels are directly related to the communication cooperation.

Another issue to be investigated is the effect of upper and lower threshold values used in distributed IDS algorithm. There is a need to optimize the lower threshold value to minimize the error rate in establishing trust levels. In simulations it is observed that the value 0.4 for lower threshold minimizes error rate. Even though this value should be thought as optimum value, changes at the network parameters and expected intrusion rate may force to reset the value. Lower values compared to higher values means more secure networks with a high error rate in establishing trust levels of nodes. Upper threshold value is up to the users. High values result in more secure networks with a higher rate of nodes having uncalculated trust levels which might not be considered as error.

Additionally, we have investigated the effects of number of intrusion instances to the system stability. An expected behavior of a malicious node is to block a network traffic having data about itself. Therefore, those malicious nodes should behave in an innocent manner to the other malicious nodes activities. For this reason, individual intrusions resulted in same consequences. However, multiple intrusion attempts originated from the same node generated more accurate reputation data and trust level assessment. Even though the proposed architecture is not designed for

cooperative intrusion attempts, local IDS engines should mitigate this vulnerability.

Because r*eputation* and *trust* are subjective concepts, it is a natural result to have different trust establishments for the same node at the network by individual nodes. However, we aim to minimize this diversity between nodes. But, we have never got 100% same trust level assessment. The aims of the network and security risks are key factors on the feasibility of the proposed architecture.

5. CONCLUSION

A trust based distributed intrusion detection framework is proposed in order to protect nodes from performing misbehavior or selfish behaviors in MANETS. In this manner, trust establishment is the major problem in proposed architecture. Reputation mechanism is used to set trust assessment, which is based on direct observations of neighboring nodes. An IDS alert message is distributed among the nodes in case of a suspicious activity and reputation data collected by watching the behaviors' of the nodes. Trust assessment is directly based on these reputation values.

For feasibility and performance analyses, we have executed several simulations. Simulation scenarios are chosen to reflect the basic characteristics of MANETs. In line with the simulations and obtained results, the proposed architecture should be feasible for networks like sensor networks, vehicular networks and networks where individual security is more important rather than military networks.

Our approach does not modify or restrict the network discovery or routing protocols. DICOTIDS is carried out at the application layer. However, simulations and the results show that, the proposed architecture needs to be integrated to network layer. In other words, untrusted nodes should be excluded and only the trusted nodes should participate in routing process. Furthermore, the distributed IDS system should be improved for collaborative intrusions. To mitigate these deficiencies, a distributed cooperative trust based intrusion architecture running on the application layer integrated to network layer, which is resistant to collaborative attacks, should be a subject to future research.

6. REFERENCES

[1] Hoebeke, J., Moerman, I., Dhoedt B. and Demeester, P., *An Overview of Mobile Ad Hoc Networks: Applications and Challenges.* Journal of the Communications Network, Vol. 3, July 2004: pp. 60-66.

[2] Sen, S. and J.A.Clark, *Intrusion Detection in Mobile Ad Hoc Networks*. Guide to Wireless Ad Hoc Networks, ISBN 978-1-84800-328-6, Springer, 2009.

[3] Indirani, G. and Selvakumar, K. *Performance of Swarm Based Intrusion Detection System Under Different Mobility Conditions in MANET.* International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Vol. 3, Issue 4, April 2013: pp. 577-583.

[4] Chhabra P., *Intrusion Detection in Mobile Ad hoc Network,* International Journal of Latest Trends in Engineering and Technology, ISSN: 2278-621X, Vol. 1 Issue 3 September 2012: pp. 34-40.

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

[6] Zhang, Y. and W. Lee, *Intrusion detection techniques for mobile wireless networks.* Wireless Networks, 9, 2003: pp. 45-556.

[7] Indirani, G. and Selvakumar, K., *Swarm based Intrusion Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks,* International Journal of Computer Applications (0975–8887), Vol. 50, No.19, July 2012: pp. 1-7.

[8] Sethi, S. and Pattnaik, A., *A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks,* Project Report, Project Id: 1236, National Institute of Science & Technology, Palur Hills, Berhampur, Odisha – 761008, India, 2012-2013.

[9] Rafsanjani, M., Movaghar, A. and Koroupi, F. *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] Sivakumar, K. and Phil, M., *Overview of Various Attacks in MANET and Countermeasures for Attacks.* International Journal of Computer Science and Management Research, ISSN 2278-733X, Vol. 2, Issue 1, January 2013: pp. 1366-1372.

[11] Vigna, G., *An Intrustion Detection Tool for AODV-Based Ad Hoc Wireless Networks.* Annual Computer Security Applications Conference (ACSAC 2004), 2004: pp. 16-27.

[12] Rebahi, Y., v. Mujica, and D. Sisalem, *A reputation Based trust mechanism for Ad Hoc networks.* 10th IEEE Symp. on Computers and Communicatins (ISCC 2005), 2005: pp. 37-42.

[13] Chen, T. and V. Venkataramanan, *Dempster-Shaffer theory for intrusion detection in mobile ad hoc networks.* IEEE Internet computing 2005, 9: pp. 35-41.

[14] Mutlu, S. and G. Yilmaz, *A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs.* The Seventh International Conference on Networking and Services (ICNS 2011), 2011: pp. 292-298.

[15] Snort, 2011 [cited 2011 30 May 2011]; Available from: www.snort.org.

[16] Hu, J. and M. Burmester, *Cooperation in Mobile Ad Hoc Networks.* Guide to Wireless Ad Hoc Networks, Computer Communications and Networks, 2009: pp. 43-53.

VITAE

Güray YILMAZ
He received his BS, MS and PhD degrees from the Istanbul Technical University in 1991, 1995 and 2002 respectively. He is currently an Assist.Prof. in Computer Engineering Department at the Turkish Air Sensor Networks.

Force Academy. He teaches Operating Systems, Parallel and Distributed Systems and Multi-Core Programming. His current research areas are Parallel and Distributed Systems, Sensor Networks, Mobile Ad-Hoc Networks, Intrusion Detection Systems and Autonomous Navigation of Unmanned Aerial Vehicles.

Süreyya MUTLU
He received his BS and MS degrees in Computer Engineering from the Turkish Air Force Academy, Istanbul, Turkey. His current research areas are Distributed Systems, MANETs and Wireless.