A P2P Fuzzy Reputation System Based on Security Policies for Mobile Ad-Hoc Networks

Morteza Romoozi and Hamideh Babaei

Abstract—**Security is one of the most challenging problems in Mobile ad-hoc networks and P2P networks. Many researches have tried to improve multi-hop networks security using different techniques. One of these methods is using reputation technique for system security. A reputation system detects malicious nodes and does not let them participate in routing and reject any request for network services. This paper enhances Gnutella content discovery protocol to a reputation system. Many reputation systems consider routing disordering as malicious behavior where this paper adds security policy violation as a new maliciously behavior. This paper present an adoptable and customizable reputation system to apply security rules on each group of the nodes. More accuracy and inability for assigning a strict level of rating to a node have been caused using a fuzzy method for rating of the nodes and determining the reputation level.**

Index Terms—**Reputation system, mobile ad-hoc networks. security policy, P2P networks trustness.**

I. Introduction

Today, security is one of the critical problems for most organizations assets that include electronically media, documents and IT services in addition to physical assets. Security is conformed from three base principles, availability, integrity and confidentiality. Each organization must consider these three principles in its security programs. One of the most important steps in the security program is establishing security policy document. Security policy includes access control licenses, security levels of media and security rules that are determined by analysis of information, process and risk analysis.

Ad-hoc networks are one of the easiest to install and use computer networks that have not a physical infrastructure. One of the base characteristics of this network is mobility of the nodes. So network topology changes continual.

On the other hand, today Peer to Peer (P2P) networks have also had considerable growth compared with client-server architectures, and have dedicated high traffic to themselves. In these networks both nodes can exchange information without any need to an infrastructure or a central node.

P2P and MANET networks have many similarities in nature, including being self-organizing and decentralized, and having dynamic topology. However, there are differences between them too [1]. For instance, topology in MANET networks is more dynamic than P2P networks due to node movement in MANET. In addition, MANET networks encounters limitations such as low computing capacity, radio transmission range, and power consumption.

The similarities between the two types of networks, the significance and simplicity of MANET deployment, and wide applications of P2P have opened a new research field that attempts to apply P2P paradigm over MANET networks. The most important application in P2P networks is content discovery. There are two types of content discovery technique. 1. Unstructured protocols and 2.Structured protocols.

In unstructured protocols, there is no specific law to define the location of stored data and network topology. They use message flooding for content discovery. Gnutella [2] and Random walk [3] are two significant protocols of this type.

Gnutella protocol distributes queries by flooding fashion. When a node receives a query, it examines whether it has the requested content or not. If it has, the node send back a message to query source; otherwise, the node sends query to all the neighboring nodes in its list. To prevent the message infinite distribution, the amount of a TTL field that exists in query message is reduced per hop. The messages which have zero amount of TTL are dropped.

In structured protocols, the neighboring connection between nodes and stored data locations are clearly defined. Chord [4] is one of the most well-known structured protocols. It uses a distributed hash table for content and file division among peers.

Security problem in MANET and P2P networks is more challenging Because of nature of this network. One of the strategies to secure MANET is detection malicious nodes and response to them and preventing to deliver network service and data to them. Such strategy is applied by Reputation Systems. Malicious nodes are nodes which do not participate in routing, or cause disorder in it, or violate security policy of organization.

This paper presents a novel reputation system which enables security policy and rules of each organization in addition to disordering content discovering or delivering process. This system is implemented in application layer and is applied on an unstructured P2P content discovery protocol which works like classic Gnutella.

In this paper after surveying related works, security policy is discussed and a method for applying it to network nodes will be proposed. Finally a reputation system based this policies will be proposed.

II. Related Works

Our paper tackle to trust problem on a P2P networks that has been implemented over a MANET. Hence in the related work we survey first, some reputation system over

Manuscript received September 25, 2012; revised December 10, 2012.

Morteza Romoozi is with Computer Eng Dept, Islamic Azad University, Kashan Branch, Kashan, Iran (e-mail: mromoozi@iaukashan.ac.ir).

Hamideh Babaei is with Computer Eng Dept, Islamic Azad University, Naragh Branch, Naragh, Iran (e-mail: hbabaei@iau-naragh.ac.ir).

MANAET and then some reputation system which is implemented on P2P networks which have a wired network as underlay structure.

As it has been studied in most papers and surveys [5], Reputation systems are classified into two groups. The first group, *one-layer* reputation *systems*, refers to those that are based on observations without an explicit evaluation of indirect observations (i.e., neighbor observations). Key examples include Watchdogs and Pathraters [6], CORE (COllaborative REputation) [7], OCEAN (Observation-based Cooperation Enforcement in Ad-hoc Networks) [8], SORI (Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks) [9], and LARS (Locally Aware Reputation System) [10]. All of them were either designed for or evaluated over DSR.

The second group, *two-layer reputation systems*, refers to those based not only on observations, but also on *trust,* which evaluates the trustworthiness of neighbor information or second-hand information. Instances of this group include CONFIDANT (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks) [11] and SAFE (Securing pAcket Forwarding in ad hoc networks) [12].

None of the mentioned systems considered security policies in reputation system. This paper presents a security policy that support reputation system.

There are several researches on reputation systems over P2P networks. One of the initial attacks against reputation system was Whitewashing [13]. But in it, Attackers reenter the network with a new identity to repair their reputation. Next, Hoffman et al. [14] improve Whitewashing reputation system by using a formulation that does not result in the same reputation for both newcomers and old peers.
In [15] a binary trust model for P2P networks has been proposed. It has been enhanced to a two-layer rating system.

III. Malicious Behaviors in Ad-Hoc Networks

Malicious behaviors can be grouped into two groups. 1. Security policy violation and 2. Routing disordering.

Security policy is a document that states in writing how a company plans to protect the company's physical and information technology assets. These policies cover all security goals such as authentication, Access Control, Confidentiality, Privacy, Integrity, Authorization, Anonymity, Non-Repudiation, Freshness and availability. Security policy specifies who and how access to what information.

Security policy violation attacks depend on security policy. It means that a behavior in an organization can be considered as an attack and in another organization as an ordinary behavior. In this paper 3 instances of this attack have been mentioned.

- Requesting or receiving confidential information that a node has no permission to request or receive it.
- Participating in routing of confidential information that node has no permission to forward it.
- Being Present in an area where node has no permission to present there.

Second group is routing disordering attacks. The routing can be considered as forwarding query in P2P content discovery technique or forwarding a packet in routing protocol in network layer. These attacks are often are active attacks. Selfish or malicious nodes try to disorder in routing deliberately. Some of these attacks are as follows:

- No forwarding (of control messages or data).
- Traffic deviation: unusual traffic attraction or the opposite (claims to have only bad routes).
- Route salvaging, i.e., rerouting to avoid a broken link, although no error has been observed.
- Lack of error messages, although an error has been observed, or vice versa.
- Unusually frequent route updates.
- Silent route change (tampering with the message header of either control or data packets).

IV. Applying Security Policies to Nodes Using Cluster Based Mobility Model

There are different types of nodes in MANET that are active in it. Each type has a movement pattern that is represented by mobility model in network simulators. Mobility model dictates to nodes how to move in their network environment. Cluster Based Mobility Model [16, 17] has been proposed by authors previously.

In this model mobile nodes are grouped in several clusters as each cluster has several common characteristics such as speed, pause time, activity area and finding path or destination method. Activity area is some areas that probability the nodes existence in those areas is more than other places. It means that nodes of a cluster are in the same position or play the same role in an organization.

Considering security problems, we can consider some other common characteristics which include security permissions driven from security policy for a cluster. These characteristics are as follows:

- Permissible activity area: the areas where cluster nodes have permission to be active.
- Permissible information for querying and receiving
- Permissible information for forwarding.

In reality we can define clusters with security permissions without considering mobility parameters.

V. Reputation System

Reputation system implements detection and response strategy against network attacks. In this system each node monitors neighbor nodes and detects its malicious behaviors and alarms to other nodes to take an appropriate reaction about malicious nodes.

This system consists of the following base components: The Monitor, the Reputation System, the Path Manager, the Policy Manager and the Trust Manager. The components are present in each node. Some of this component are the same with CONFIDENT but detail of its implementation is different.

A. Monitoring Component

This component is the heart of a reputation system. Each node monitors neighbor's behaviors and when it detects a malicious behavior, first calls its reputation component and

then generates an alarm message and sends it to its friends. Friends of each node are the nodes that are in the same cluster. We implement detection controls of all mentioned security policy violation attacks and 'No forwarding' attack from routing disordering group.

Each node implements 'No forwarding' detection by sniffing its radio range, so if its neighbor receives a packet and does not forward it, the node can detect it.

To detect security policy violation, each node should be able to answer three questions:

1) Does its neighbor attend at permissible area?
2) Does its neighbor receive or request for permissible information?
3) Does its neighbor participate in forwarding and routing permissible information?

Each node knows cluster ID of its neighbor. This ID exchanges among neighbors by Hello packets in routing protocol. For preventing a node uses of cluster IDs of other cluster maliciously, each node send hashed value of its cluster ID using classic hash method such as MD5. Thus when a node receive a hashed value of cluster ID of its neighbor, it hashes its cluster ID and compare it to received hash value. If the comparison result was equal, the neighbor node has the same cluster ID as itself.

If cluster ID of the neighbor node is the same as the node, so it will be able to answer these questions. Because each node knows security characteristics of its cluster. But if the cluster ID of the neighbor node is different, it needs to ask the answer of these questions from policy manager component. This process is described in next section.

Retrieving this information through networks puts overhead burden on the network, but it does not usually happen, because each cluster has its activity area and the nodes of a cluster are active in these areas more than other places. So neighbors of a node are in the same cluster with the node and there is no need to retrieve answers of mentioned questions through the network

B. Policy Manager Component

This component is implemented distributed and hierarchically. It means that root peer has all details of security policy documents and it determines how much of policies can be shared with its children. This process applies to lower levels. Queries to policy manager is delivered bottom-up like, meaning that each query first delivers to lowest level and if it can not reply to the query, it forwards the query to upper levels.

This component has the important duty of responding to queries that are originated by monitor component. These queries are about three mentioned questions. These queries are composed of three triplet segments. The first segment is made up of cluster ID, exposure area of neighbor node and response of policy manager. The second segment is made up of cluster ID, label of data that neighbor node will receive or request and response of policy manager. The third segment is composed of cluster ID of neighboring node, label of data that neighbor node will rout and response of policy manager.

When policy manager receives such query, if it can reply to requested question, it fills response section of each segment of received packet; otherwise it forwards received packet to higher levels of policy manager.

C. Trust Manager Component

This section is implemented adoptable and distributed. This component manages incoming and outcoming alarm messages. An alarm is originated when monitoring component of a node detects a malicious behavior of its neighbors. These alarms are distributed among the nodes which are in the same cluster with the detector node. When a malicious behavior is occurred in an area, its consequences are related to the nodes which belong to that area. On the other hand, the nodes which are active in an area are in the same cluster, so it is better that the alarms are sent to the cluster nodes.

Trust manager validates incoming alarms to be from a valid node. In fact this section validates the nodes in reputation system, but reputation system validates the nodes in routing.

This component is implemented by the same technique that is used in monitor component for exchanging cluster IDs. As mentioned, alarm messages are distributed among the nodes which have the same cluster IDs. Hence when a node originates an alarm message, inserts its hashed cluster ID value in the alarm message and broadcasts it. Each receiver, first extract this hashed value and compare it with its hashed cluster ID. If they were equal, the message has come from the right peer.

In this scenario, we assume that if a node has a right cluster ID, it can be assumed as a trusted peer. In fact, cluster ID is a secure key that is granted to each peer by its company.

D. Reputation System

Reputation systems are used in social networks or auction system to validate participants for each others. This system gives a rate to each participant that is its reputation level. So this system can be applied on content discovery protocol in MANET. Using it, mobile nodes can be validated to participate in routing a query and its response.

This component is called when an alarm is received by a node or when a node detects a malicious behavior. This alarm is delivered to this component after validation by trust manager. Reputation system gathers these alarm messages and makes a history of malicious behavior. This history is perused in predefined period.

Each malicious behavior has specific impact and frequency. So they must be considered in validation of the nodes. The impact of a malicious behavior is the consequences of it for organization.

Rating systems are grouped into two binomial and multinomial groups. Binomial rating systems have two levels, good and bad. But in multinomial rating system, there are multi levels for rating. As it has been mentioned, there are variant types of malicious behaviors with variant frequencies. Hence multinomial rating system is more suitable than binomial.

However because of variable frequency and variant malicious behavior impact, it is very hard to match the rating of a node to the predefined levels. It means the rating of a node can be between two levels. For example, if there are 2 levels of rating in a system, bad and good, value of rating a node may be calculated between of two levels, not

exactly good and not bad. Therefore rating level can be defined as fuzzy problem. So a fuzzy member function can be assigned to each rating level. To this end, four Gaussian fuzzy rating level member functions are applied.

For example Fig. 1 illustrates these member functions. There are four fuzzy diagrams; each of them represents a rating level. In some points the diagrams have subscription to each other. It means in some points rating of a node can belong to two levels.

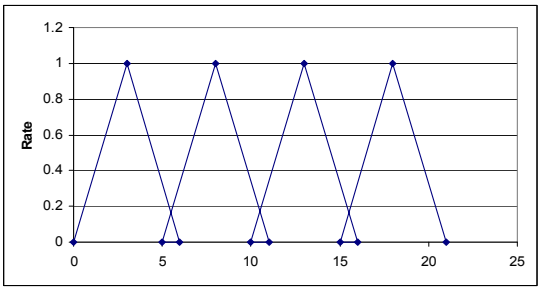

Fig. 1. Fuzzy rating levels

Each malicious behavior has a fuzzy member function that has two important parameters. The first parameter is impact parameter that each organization can set based on importance of the malicious behavior for the organization. The second parameter is frequency of the malicious behavior.

Below formula is used as member function for all behaviors.

$$\mu(I, f) = \frac{1}{e^{1/I + f}} \tag{1}$$

E. Fuzzy Control System for Rating

This system has n pairs of inputs, Fuzzifier, fuzzy rules base knowledge base, an inference engine, Defuzzifier and an output as real number.

1) *Inputs*: input is n pairs (behavior, frequency) that are entered as the real numbers. For example an input as (2,2/(2+3)) means behavior number 2 with frequency 2 times from 2+3 times. There are n inputs for n possible types of malicious behavior that a node may committ.

2) *Fuzzifier:* Fuzzifier is employed as a map from a real point to a fuzzy set. Gaussian fuzzifier has been employed to bring real numbers to a fuzzy set. The formula below represents this fuzzifier. 'a' is a positive parameter and x^*_i is the inputs of the fuzzier.

$$\mu_{A'}(X) = e^{-\left[\frac{x_1 - x_1^*}{a_1}\right]_2} \times \ldots \times e^{-\left[\frac{x_n - x_n^*}{a_n}\right]_2} \tag{2}$$

3) *Rule based knowledge base:* this knowledge base is filled based on security policies. Each rule brings combination of input fuzzy set to an output fuzzy set. So each rule has the structure below. A_i is input fuzzy set which represents n different fuzzy malicious behaviors. B_j is output fuzzy set which represents k rating level fuzzy sets.

If x_1 *is* A_1 and x_2 is A_2 and …and x_n is A_n then y *is* B_j

4) *Inference Engine:* product inference engine is used. inference is based on separated rules with union combination, mamdani product inference, algebra product for t-norms and maximum for s-norms.

5) *Defuzzifier:* Defuzzifier is a map from output fuzzy set of the inference engine (B') to an absolute real point ($y^* \in B$). Center Average Defuzzifier has been employed. Below formula describes this defuzzifier. Output of the folowing formula is considered as rate for the node.

$$y^* = \frac{\sum_{l=1}^{M} \bar{y}^l w_l}{\sum_{l=1}^{M} w_l} \tag{3}$$

F. Path Manager Component

As it is mentioned, Gnutella distributes queries by flooding fashion. When a node receives a query, it examines whether it has the requested content or not. If it has, the node send back a message to query source; otherwise, the node sends query to all the neighboring nodes in its list. To prevent the message infinite distribution, the amount of a TTL field that exists in query message is reduced per hop. The messages which have zero amount of TTL are dropped. The path manager is called when a decision is supposed to be made about routing a query or its response. The path manager performs the following functions:

- Action on receiving a query from a malicious node.
- Action on receiving a response packet by malicious nodes.
- Action on receiving a forwarded query from malicious nodes.
- Action on receiving a forwarded response packet by malicious node.

Being malicious or not is specified by reputation system. This path manager system makes one-hop decisions. It means, in each hop, if a malicious behavior is detected, procedure is stopped.

VI. Simulation

The objective of performance analysis is to determine the impact of the new reputation system in the P2P content discovery protocol, Gnutella which is implemented over a MANET while part of the population acts maliciously.

A. Simulation Metrics

To determine the impact of new protocol on the performance of P2P content discovery protocols, the Gnutella protocol is utilized for content discovery and delivery. To this end, the following metrics will be evaluated:

1) Hit Rate; the number of queries that are responded successfully.
2) Average Response Times: the amount of time that a user should keep waiting for receiving the required response to its query. The time contains the amount of time needed for query transmits in the network, discovering the target content, and returning the response back to the user.
3) Average Energy Consumption: the average energy that a node consumes during simulation for sending and receiving signals, even in idle status.

B. Simulation Setup

For the performance analysis of the protocol extensions, the metrics are observed in various network scenarios given by different modifications of the Gnutella protocol. The first network we analyze is a regular well-behaved Gnutella network which is used as a reference.

We then introduce compromised nodes that do not cooperate. These malicious nodes do not forward messages to other nodes. Furthermore these malicious nodes deny organization policy in requesting and receiving contents and presenting in unpermitted area.

The next kind of network we use for analysis is a network containing a certain fraction of malicious nodes but with no defense mechanism, we call it `defenseless'.

Then we use a version of Gnutella that we enhanced with proposed reputation system extensions and refer to it as `Reputation Support'.

C. Simulation Parameter,Terrain and Clusters

Fig. 2 illustrates the network terrain which contains obstacles and pathways to evaluate new protocol. Table I lists other simulation parameters.

TABLE I: SIMULATION PARAMETERS

Parameter	Value
Simulator	Ns-2 network simulator
Simulation terrain size	1000m x 1000m
Maximum node transmission range	250m
Propagation model	two-ray pathloss model
MAC layer protocol	IEEE 802.11 DCF
Bandwidth	2Mbps
Speed range	[0…2m/s]
Pause time range	[10…300s]
Number of Nodes	50
Routing Protocol	AODV [18]
Traffic Model	CBR (20 Data session with 6000 bytes per session and sending rate 4 packet/second.)
Simulation Time	1800 s

TABLE II: CLUSTER DEFINITION

	Cluster #1	Cluster #2	Cluster #3	Cluster #4	Cluster #5
Activity area	1	2	3	Total	Total
Speed range	0-2 m/s	0-3 m/s	0-4 m/s	0-2m/s	4-10 m/s
Pause time range	30-400 s	10-300 s	200-1000 s	50-200 s	10-100 s
Maximum capacity	10%	35%	25%	25%	5%
Permissible Areas	Total	2,1	3,2	2,3	1,3
Permissible Data to Request	Protected	Confidential	Restricted	Confidential	Public
Permissible Data to Route	Protected	Restricted	Protected	Restricted	Confidential

Five clusters have been defined (Table II) for simulation. These clusters have different mobility characteristics and security permissions. Information is classified and labeled. For example 4 labels can be considered, Protected, Restricted, Confidential and Public.

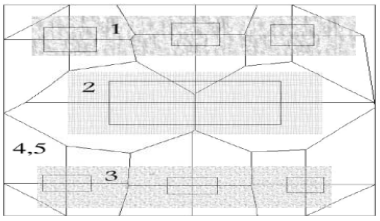

Fig. 2. Activity area of clusters 1, 2 and 3

In Gnutella it is assumed that each node has maximum six neighbors. TTL of each query is set to 4, and ping messages are sent every 10 seconds.

D. Simulation Results

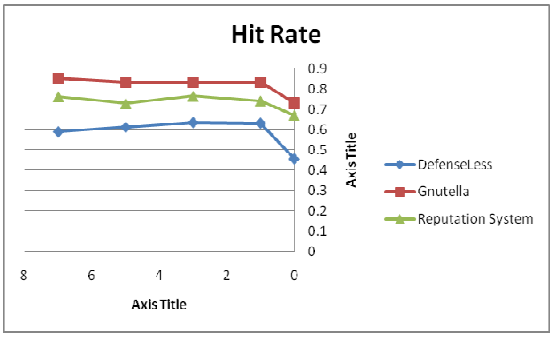

Fig. 3. Hit rate

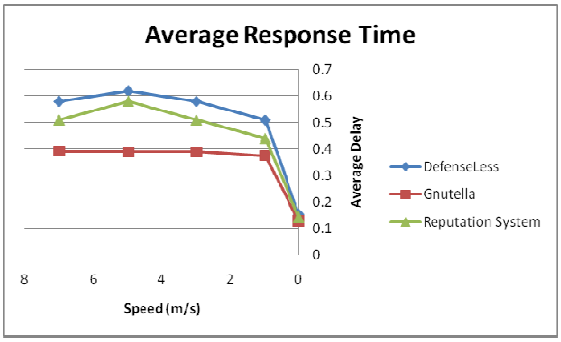

Fig. 4. Average response time

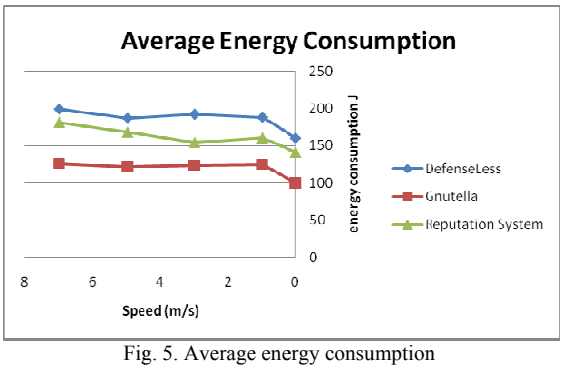

Fig. 5. Average energy consumption

Hite Rate: Best result in Fig. 4 is related to classic Gnutella with no malicious nodes. When malicious nodes are active on the network, they disorder in routing and forwarding query packets. So hite rate is decreased.

But when reputation system is added, it cannot neutralize malicious nodes impact completely. It can be result of some policy violation behaviors. It means some nodes request some data for which they have not permission to request, so this data cannot be delivered to them and leads to the less hit rate than Gnutella with no malicious nodes.

Average Response Time: Fig. 5 illustrates average

response time. Average response time of Gnutella whith out malicious nodes is less than other models. But when malicious nodes are added, they cause to drop some query and response time is increased. When reputation system is used, it prevent forwarding a query to a malicious node and therfore response time is decreased. But when reputation system control policy violation of the malicious nodes, some query dropped and response time is increased.

Average Energy Consumption: Average energy consumption of clasic gnutella is less than other diagrams according Fig. 5. It is as result of lacking malicious nodes. When the malicious nodes are active and there is no defense against them, energy consumption is increased. Because some queris need to regenerate and reforward due dropping them. Reputation system try to control malicious nodes and do not forward query and response packet to them. It can save energy consumption. But dropping packet due security policy violation cause to more energy consumption than classic Gnutella.

VII. Conclusion

This paper presented a reputation system based on security policies which is implemented over MANET. We used a policy manager component to apply security policies. This component implemented and distributed completely. Each node knows its permission which is a part of policy manager. Also, there are some other nodes in role of policy manager which have hierarchy structure. Using such structure is enabled organizations to apply their policies hierarchically. So there is no need to some non permissible node to know confidential policy document to perform security policy violation prevention.

Proposed reputation system has used a fuzzy expert system for rating of the nodes. Using such system, we can import some security rules to knowledge base and use them for rating of the nodes. Hence reputation of a node is affected by security policies. Besides using a fuzzy system helps this system for more accurate rating.

Simulation results show that using this system can control malicious behaviors and inactive them. But using this system put more control packets burdens network than normal situation.

References

[1] L. B. Oliveira, I. G. Siqueira, and A. A. F. Loureiro, "On the performance of ad hoc routing protocols under a peer-to-peer application," *Journal of Parallel and Distributed Computing*, vol. 65, no. 11, 2005.

[2] A. Boukerche, A. Zarrad, and R. Arajo, "Smart Gnutella overlay formation for collaborative virtual environments over mobile ad-hoc networks," in *Proc. Tenth IEEE International Symposium on Distributed Simulation and Real-Time Applications (DS-RT)*, 2006, pp. 143–156.

[3] C. Gkantsidis, M. Mihail, and A. Saberi, "Random walks in peer-to-peer networks," in *Proceedings of the IEEE Infocom*, 2004, pp. 130

[4] I. Stoica, R. Morris, D. L. Nowell, D. R. Karger, M. F. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: a scalable peer-to-peer lookup protocol for internet applications," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, 2003, pp. 17–32.

[5] P. Ning and K. Sun, "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols," *Ad Hoc Networks*, vol. 3, no. 6, pp. 795–819 , 2005

[6] K. Lai, M. Baker, S. Marti, and T. Giuli, "Mitigating routing Misbehavior in mobile Ad hoc networks," in *Proceedings of MOBICOM* , pp. 255–265, 2000.

[7] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *IFIP TC6/TC11 6th Joint Working Conf. on Comm. and Multimedia Security: Adv. Comm. and Multimedia Security*, pp. 107–121, 2002.

[8] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," *Technical Report CS/0307012*, Stanford University, 2003.

[9] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputation-based incentive scheme for ad hoc networks," in *IEEE Wireless Communications and Networking Conference*, (Atlanta, GA, USA, 2004.

[10] J. Hu and M. Burmester, "A locally aware reputation system for mobile ad hoc networks," in *Proc. of the 44th Annual Southeast Regional Conference*, pp. 119–123, 2006.

[11] S. Buchegger and J. Y. L Boudec, "Performance analysis of the CONFIDANT protocol," in *Proc. 3rd ACM Int. Symp. on Mobile Ad Hoc Network & comput*, 2002, pp. 226–236

[12] Y. Rebahi, V. Mujica, C. Simons, and D. Sisalem, "SAFE: Securing pAcket Forwarding in ad hoc nEtworks," in *Proc. 5th Workshop on Applications and Services in Wireless Networks*, 2005.

[13] F. G. M´armol and G. M. P´erez, "Security threats scenarios in trust and reputation models for distributed systems," C*omputers & Security*, vol. 28, no. 7, Oct. 2009, pp. 545-556,

[14] K. Hoffman, D. Zage, and C. N. Rotaru, "A Survey of Attack and Defense Techniques for Reputation System," *ACM Computing Surveys*, vol. 41, no. 1, pp. 1-31, Dec. 2009

[15] K. Aberer and Z. Despotovic, "Managing trust in a peer-2- peer information system," in *Ninth International Conference on Information and Knowledge Management (CIKM)*, Nov. 2001.

[16] M. Romoozi, H. Babaei, and M. Fathy, "A Cluster-Based Mobility Model for Intelligent Nodes," in *ICCSA* 2009, Part I, LNCS 5592, 2009, pp. 565-579.

[17] H. Babaei, M. Fathi, and M. Romoozi, "Obstacle Mobility Model Based on Activity Area in Ad hoc Network," in *ICCSA*, LNCS 4706, Part II, 2007, pp. 804–817.

[18] C. E. Perkins, E. M. B. Royer, and I. Chakeres, "Ad Hoc On Demand Distance Vector (AODV) Routing," *IETF Internet draft*, 2003

Mortreza Romoozi is currently PhD student at Science & research branch of Islamic Azad University in Iran. He received Bs in software engineering from the University of Kashan at 2003, and his MS in computer science at 2006 in Iran. He is a faculty member of Islamic Azad University (Kashan branch). He has taught in the areas of Wireless Networks, Ad hoc and P2P Networks and his research interests include Semantic Web, Information Retrieval, and recent research focusing on the Mobility model and routing protocol in ad-hoc networks. He has published several articles in international conferences, LNCS series and other springer journals.

Hamideh Babaei received PhD in computer networks from Science & research branch of Islamic Azad University in Iran. She received Bs in software engineering from the University of Kashan at 2003, and his MS in computer science at 2005 in Iran. She is a faculty member of Islamic Azad University (Naragh branch). She has taught in the areas of Wireless Networks, Ad hoc and Sensor Networks and her research interests include Semantic Web, Information Retrieval, and recent research focusing on the Mobility model and routing protocol in ad hoc networks. She has published several articles in international conferences, LNCS series and other springer journals. Email: hamidehbabaei@yahoo.com