

## Message Security in Mobile Ad-Hoc Networks

### Prayag Narula

Division of Information Tech.  
Netaji Subhas Institute of  
Technology  
University of Delhi  
India  
prayag@coe.nsit.ac.in

### Sanjay Kumar Dhurandher

Division of Information Tech.  
Netaji Subhas Institute of  
Technology  
University of Delhi  
India  
sdhurandher@coe.nsit.ac.in

### Sudip Misra

Department of Computer  
Science  
Yale University  
New Haven, Connecticut  
USA  
sudip.misra@yale.edu

### Isaac Woungang

Department of Computer  
Science  
Ryerson University  
Toronto, Ontario  
Canada  
iwoungang@scs.ryerson.ca

### ABSTRACT

Due to their applications in situations such as emergencies, crisis management, military and healthcare, message security is of paramount importance in mobile ad-hoc networks. However, because of the absence of a fixed infrastructure with a designated centralized access points, implementation of hard-cryptographic security is a challenging prospect.

In this paper, we propose a novel method of message security using trust based multi-path routing. Less trusted nodes are given lower number of self-encrypted parts of a message, making it difficult for malicious nodes to gain access to the minimum information required to break through the encryption strategy. Using trust levels, we make multi-path routing flexible enough to be usable in networks with 'vital' nodes and absence of necessary redundancy. In addition, using trust levels we avoid non-trusted routes that may use brute force attacks and may decrypt messages if enough parts of the message are available to them.

**Keywords:** MANETs, Multi-path, Trust, Encryption

### 1. INTRODUCTION

Mobile ad-hoc networks are wireless and do not require any infrastructure to set up. This makes them ideal for military, rescue and relief operations. But this flexibility and the lack of a central server or access point creates a problem of message security. Since the nodes co-operate to route messages the message security cannot be implemented without a message encryption strategy. Traditional key-based encryption techniques require certification authorities and key distribution centers to trustfully transfer keys between nodes. This requires a centralized or partially distributed authorization, which is again difficult to achieve, in the infrastructureless and improvised environment of ad-hoc networks.

We propose a method to securely route messages in an ad-hoc network using multi-path routing and trustworthiness of the nodes. We divide the message into different parts and encrypt these parts using one another [1]. We then route these parts separately using different paths. An intermediate node can access different parts on the basis

of its trustworthiness. That is, a more trusted node is allowed to feature in more paths than a less trusted node and hence access to more message parts than a less trusted node. This feature allows the routing algorithm to avoid nodes that are more likely to attempt 'breaking-in' the encryption. In addition, suspected nodes which have high computation power and are hence likely to be more successful in cryptanalysis can be given less parts to stymie their plans.

Since establishment of trust also requires cryptographic key exchange, we use a soft approach to trust [2]. Trust levels of peer nodes of the network are found using effort-return based trust model [3]. We use a variation of the model given in [3] and [4], which uses a combination of *derived trust and reputation* to estimate trust values of a node.

In sum, our contributions are as follows:

- We combine multi-path routing and trust with soft encryption technology to propose a scheme which is much more secure than traditional multi-path algorithms.
- Our algorithm even works in the cases where a 'vital' node is present in the network structure, unlike most other multi-path security algorithms. This point is explained in the next section.
- We provide 'soft' encryption by using the message itself for encryption. This technique eliminates the need of Key Distribution Centers and key transfer.

### 2. PREVIOUS WORKS

Various different protocols used for secure routing in mobile ad-hoc networks can be roughly categorized into following categories:

1. Payment Systems.
2. Reputation Systems.
3. Cryptography based systems.

Payment systems such as Nuglets[5] are based on the principle of providing economic incentive to the user for co-operating with other nodes in the network. Packet Trade Model (PTM) and Packet Purse Model (PPM) are two models used for charging for services by the nodes.

The payment model is an effective model if a special tamper proof hardware or a central authority server

is available to ensure that the behavior of the node and the charge and credit to each node is not modified. This is not always a valid assumption. Nonetheless, payment systems provide a model which appeals to the basic human emotion of incentive to the node for co-operation, either economic or otherwise.

Reputation System such as CONFIDANT[6], are based on the principle of reputation to combat the misbehavior of the nodes. It is usually implemented as an extension to the existing on-demand models. Misbehavior is detected and punished by decrementing the reputation of the agent, which results in some of the privileges being taken away. On the other hand benevolent behavior is rewarded by some additional privileges. This model has been implemented in various different environments and has been emulated in the mobile ad-hoc networks with reasonable effectiveness. Systems such as CORE (COLlaborative REputation mechanism)[7] implement node co-operation on the basis of collaborative monitoring techniques.

Cryptography based systems such as ARIDANE[8], SRP[9] and ARAN[10] use cryptographic techniques for implementing security in mobile ad-hoc networks. They have an added advantage of being able to cope up with Denial of Service (DoS), message modification and fabrication attacks. But most, if not all, cryptographic systems assume effective key distribution system which is really difficult to achieve in the dynamic topology of mobile ad-hoc networks. Moreover, most cryptographic systems are resource intensive and are difficult to implement using software and hence are difficult to use in the resource limited devices that generally partake in mobile ad-hoc networks.

### 3. MOTIVATION

Multi path routing has been traditionally used in wired networks for providing various QoS guarantees [11]. A lot of work has been done on using multiple paths to secure message transfer. But most of the algorithms are based on just routing different parts of the message using different paths [12]. Most of these algorithms depend on finding  $k$  disjoint paths between the source and destination, where a message is divided into  $n$  parts, where  $n > k$ . There may not be enough redundancy in the network. In addition, there may be a *vital* node in the network which exists in all the valid paths. In such a scenario, these algorithms would not work even if the vital node is a trusted node and allowed access to the complete message. A sample topology of such a case is shown in Figure 1.

In a topology similar to Figure 1, even if we are sure about the non-malicious intent of node D, no secured routing can be done to the nodes A to G since no disjoint paths can be found from node A to G.

In most of the multi-path algorithms, it is often trivial to get access to at least some parts of the messages. Since neither of these algorithms do not take into account the possibility of some of the nodes being more malicious

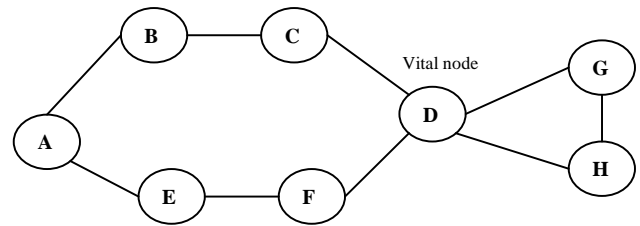


Figure 1: No disjoint path to node G

than other, either due to intent, or due to capability (certain nodes may have more computation power to be able to perform more successful brute force attacks). Hence, these algorithms make message parts available indiscriminately, making most of these algorithms vulnerable to brute force attacks especially when a large part of the message is available to a compromising node. Hence, it is important to take into account the trustworthiness of the nodes and route the message parts accordingly. This would make multi-path routing algorithms more flexible by allowing a complete message to be routed via the trusted nodes, if required. In addition, this would also help in limiting data access to nodes more likely to carry out brute force and other attacks and if the trust level is low enough in avoiding them completely.

#### Message Encryption

Most of the encryption-based security techniques are based on secured key exchanges. *A priori* negotiations are required for key exchanges in dynamic ad-hoc networks. Pre-shared keys are used in networks which are less dynamic in nature [13]. Such networks are sometimes called “managed ad-hoc networks” [4].

Ref. [15] uses a distributed approach in which multiple nodes collaborate to act as a Certification Authority [1]. It uses a message encryption technique in which each part of the message is involved in encrypting the whole message itself. This avoids the problem of key exchange as the message parts are themselves used as the keys. This encryption technique is used in this paper.

#### Trust Establishment

The authors of [4] state that all the trust establishment protocols depend on a Central Trust Authority. Ref. [2] presents a distributed model based on peer recommendation. The authors define trust as a subjective entity which is transitive in nature under certain stated conditions. It generalizes the notion of trust and defines a complete trust model in which different nodes give a subjective, discrete and dynamic trust values to their peers based on repeated interactions. Refs. [3] and [4] define a trust model explicitly for mobile ad-hoc networks. They give continuous and normalized trust levels depending on the benevolent behavior shown by the nodes. The authors

use the Dynamic Source Routing (DSR) protocol [14] for routing via the trusted nodes only [15].

#### 4. PROPOSED ROUTING STRATEGY

##### 4.1 Trust

We use a variation of the trust models used in [2] and [3] in our algorithm. A node is assigned a discreet trust level in the range of -1 to 4. A trust level of 4 defines a complete trust and a trust level of -1 defines a complete distrust. These trust levels also define the maximum number of packets which can be routed via those nodes. A trust level of -1 signifies that any packet coming from that node should be dropped. No packet is in turn routed to these nodes leading to an isolation of malicious nodes..

##### 4.2 Trust Levels assignment

The trust level assigned to a node is a combination of direct interaction with its neighbors and the recommendations from its peers. A node assigns a direct trust level to its neighbor on the basis of acknowledgements received. If the neighbor sends a prompt acknowledgement of the packet received, it is assumed that the node is not involved in a resource intensive brute-force attack and hence is assigned a higher trust level. The direct trust is then combined with the trust recommendation from its peers and a final trust level is assigned to it. Note that these trust levels are assigned dynamically and are cached by a node for performance enhancement. The trust recommendations are piggybacked on DSR routing packets that is explained later in Section 3.5.

Consider Figure 2.  $T_{xy}$  represents the direct trust in node Y by node X.  $T_{yz}$  represents the trust recommended by the node Y in node Z. If  $T'_{xz}$  represents direct trust of node Z in node X, then the trust assigned by X in Z is given in Equation (1), and is available in Ref. [3].

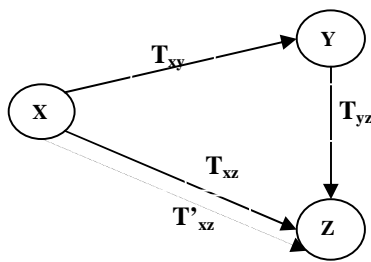


Figure 2: Direct and Derived Trust

$$T'_{xz} = 1 - (1 - T_{xz}) \cdot (1 - T_{xy}) \quad (1)$$

where,

$$T_{xyz} = 1 - (1 - T_{xy})^{T_{yz}} \quad (2)$$

The trust levels are normalized to integer values using standard methods. Each node is given an integer trust value lying between -1 to 4.

##### 4.3 Message Encryption and Routing

We use the message encryption proposed by the authors in [1].

A  $4n$  bits message is divided into 4 parts which are  $n$  bits long. Let us denote these parts by  $a$ ,  $b$ ,  $c$  and  $d$ . We define the bit operation XOR on a bit vector  $k$  and  $l$  such that

$$\begin{aligned} \text{if } & k = \{k_1, k_2, k_3, \dots, k_n\} \\ \text{and } & l = \{l_1, l_2, l_3, \dots, l_n\} \end{aligned}$$

then

$$k \text{ XOR } l = \{k_1 \text{ XOR } l_1, k_2 \text{ XOR } l_2, k_3 \text{ XOR } l_3, \dots, k_n \text{ XOR } l_n\} \quad (3)$$

We divide a  $4n$ -bit message into 4  $n$ -bit parts ( $a, b, c$  and  $d$ ) and encrypt them using the following equations:

$$a' = a \text{ XOR } c \quad (4)$$

$$b' = b \text{ XOR } d \quad (5)$$

$$c' = c \text{ XOR } b \quad (6)$$

$$d' = d \text{ XOR } a \text{ XOR } b \quad (7)$$

The parts  $a'$ ,  $b'$ ,  $c'$  and  $d'$  are now routed instead of  $a$ ,  $b$ ,  $c$  and  $d$ . Paths between the source and destination nodes are found using DSR. A node waits for intermediate multiple paths to the destination. Routing paths are selected from the set of paths using a novel *trust defined strategy*, which is described in Section 3.4..

##### 4.4 Trust Defined Strategy:

We define the Trust Defined Strategy to secure routing as the policy in which a node with a trust level of  $x$  is given at most  $x$  parts of the packet to forward. This limits the possibility of a brute force decryption of the message. For example, if the nodes are assigned 4 levels of trusts (trust 1-4) excluding no trust and complete distrusts (trust level of 0 and -1), the message would be divided into 4 parts Hence,

- A. A node with a trust node of 4 can read the message. Hence, only those nodes that have been certified to be completely safe can be given the right to read the full message. These might include nodes which are directly visible in case of military applications or nodes with which keys have been exchanged securely.
- B. A node with a trust level of 3 can be sure of finding  $2^n$  possible messages of which one would be correct, where  $n$ = no. of bits used for encryption. For example, if a 32-bit message is sent as four 8-bit messages, then a node with trust level 3 would receive 3 bytes and assuming the remaining byte (out of 256 possibilities through brute force), it can find the entire message.

- C. Using the similar process, A node with a trust level of 2 can be sure of finding  $2^8 * 2^8$  possible messages.
- D. Similarly, a node with a trust level of 1 can be sure of finding  $2^8 * 2^8 * 2^8$  possible messages.
- E. A node with a trust level of zero is not given any parts of the message. These are the nodes that are acting as sink and are not forwarding any messages or the nodes that mangle the messages before forwarding.
- F. A node with trust level of -1 is a certified malicious node. All packets received from these nodes are dropped immediately. Measures are taken to limit any promiscuous access of message parts by this node.
- G. Hence the probability of comprehending the entire message decreases by a factor of  $2^n$  as the trust level decreases.

At destination, the message parts can be decrypted using the following equations:

$$a = b' \text{ XOR } d' \quad (8)$$

$$b = a' \text{ XOR } b' \text{ XOR } c' \text{ XOR } d' \quad (9)$$

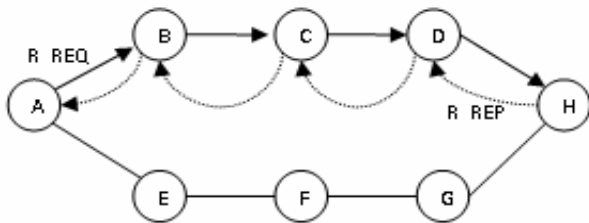
$$c = a' \text{ XOR } b' \text{ XOR } d' \quad (10)$$

$$d = a' \text{ XOR } c' \text{ XOR } d' \quad (11)$$

#### 4.5 Implementation using DSR

DSR is an on-demand routing protocol. We implement our algorithm over DSR since it is capable of finding multiple routes between the source node and the destination node.

When a node wants to route a message securely to a destination it broadcasts a Route Request packet (R\_REQ). If this packet reaches the destination or a node which has a path to the destination in its cache, it sends a Route Reply (R\_REP) to the source. The R\_REP message is appended with the trust level of the previous node by the node sending the route backwards along a path.



**Figure 3:** DSR Routing Protocol

For example, in the network represented in Figure 3, the R\_REP packet sent by the destination node H contains the

path {A,B,C,D,H} back to the source node A using the path in the reverse. When the packet reaches node C, it appends to it a trust value in the packet for D. Similarly, B appends the trust value of C.

Node A can also explicitly request the trust values of nodes lying in the path from other nodes in the network by sending a recommendation request as explained in Ref. [2].

#### 4.6 Route Selection

Whenever a new path is discovered and the trust levels of the nodes involved are available, efforts are made to select a secure route. The routes are selected using a greedy approach on the basis of path length such that a node with a trust level  $T$  does not get more than  $T$  packets on the route.

Figure 4 presents the algorithm used for selecting routes to securely route the data from source to destination.

### 5. SIMULATION AND RESULTS

The simulation experiments conducted were evaluated in Global Mobile Information System Simulator (GloMoSim) [17].

```

Arrange the paths  $P = \{P_1, P_2, P_3, \dots, P_n\}$  in increasing order of path length

Initialize Count  $C_i$  for all nodes = 0

Select smallest path from  $P\{$ 
  Select next smallest path
  if( for all selected nodes  $i C_i \leq T_i\{$ 
    if( four paths selected)
      break out of loop;
    else
      continue;
  }

  if(all paths exhausted)
    wait for another path
}

if (no paths left)
  Print("Not possible to route securely")
  
```

**Figure 4:** Algorithm to select secure routes

GloMoSim is a scalable simulation environment for large wireless and wireline communication systems using parallel discrete-event simulation language called PARSEC [18]. It is assumed that the trust levels of various nodes would be available to the source node via piggybacking the recommendations on the route response packets. To avoid complexity, each node randomly assigns trust levels to its peers. This is done in such a manner that most nodes have trust levels of either 2 or 3. Lesser number of nodes have trust level of 1 and even lesser number of nodes have a trust of 0 or 4. Very few nodes have a trust level of -1. A

comparison was done with the algorithm used in [1] and normal DSR-based routing.

### 5.1 Set Up

The number of nodes was varied in a terrain measuring 2000m x 2000m. To maintain connectivity, radio transmission power was varied accordingly. The MAC protocol used is IEEE 802.11 [19]. Nodes were placed uniformly throughout the terrain and simulation was allowed to run for 600 seconds.

### 5.2 Parameters

The algorithms were compared on the parameters measuring *security* and *route selection time*. Security was measured on the basis of access violation of the trust defined strategy, that was presented in Section 3.4.

*Trust compromise* is the total sum of access violation in all the paths used for routing. *Access violation* is the difference between the number of packets a node gets and the trust level of that node, if the trust level is lesser than the number of packets. Formally, if  $S$  denotes the set of nodes used for routing, then for a node  $s$  with assigned trust  $T_s$  by the source, if  $s$  receives  $N_s$  different packets from all routes,

$$\text{Trust Compromise} = \sum_{s \in S} (N_s - T_s); \text{ where } N_s > T_s \quad (12)$$

The total trust compromise is calculated for all the paths selected for routing. Since, normal DSR uses single path to route a message therefore only one path is considered in DSR. It is clear that more the trust compromise for a path set, the lesser is the message security. Ideally, the trust compromise of a path should be zero to make sure that only minimal access is given to the peer nodes to a message. The more is the trust compromise, the higher is the probability of a message to be compromised and broken by a malicious agent. The summing up of individual trust compromises models the co-operation that may be taking place between the malicious nodes. For example, if a message has a compromise of 4 and if each compromise takes place at a separate node for a separate message part, the whole message can be read if the malicious nodes are co-operating. Similarly, higher the aggregated trust compromise, the more are the chances of a message being broken into by the compromising and co-operating malicious agents.

*Route selection time* is defined as the total time required for selecting a path set for routing. Since, DSR uses the first path it receives; its path selection time is the time taken in getting the first route reply.

### 5.3 Results

The performance comparison is done in between the algorithms on the basis of the parameters stated above. The results are indicated in the plot shown in Figure 5. Since, trust based multipath routing selects a route such that no node receives more parts of a message than its trust level; it has a trust compromise of zero in all cases. Moreover, since multipath routing using 2 disjoint paths sends message

along different disjoint paths its trust compromise is zero when all the involved nodes have a trust level of more than

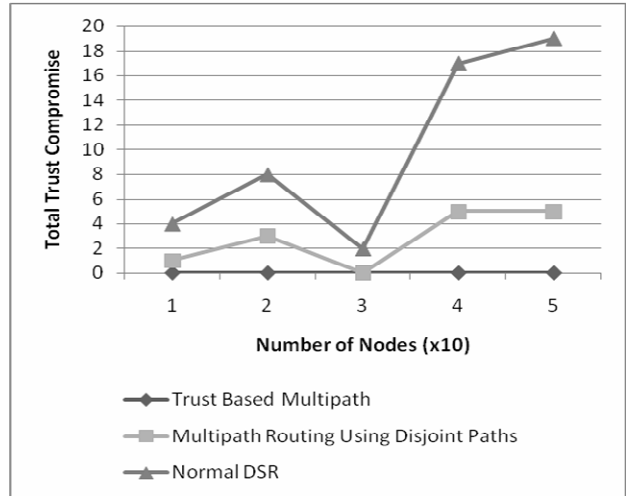


Figure 5: Comparison of Trust Compromise

or equal to 2. But since that may not necessarily be the case, trust compromise for such an algorithm varies between 0 and 5 in the results. In addition, since the DSR routes a message via the first message it gets, the message security in DSR is minimal, as compared to other algorithms. The trust compromise for the normal DSR varies from 2 to 14 in the observed results.

The route selection times for the three algorithms

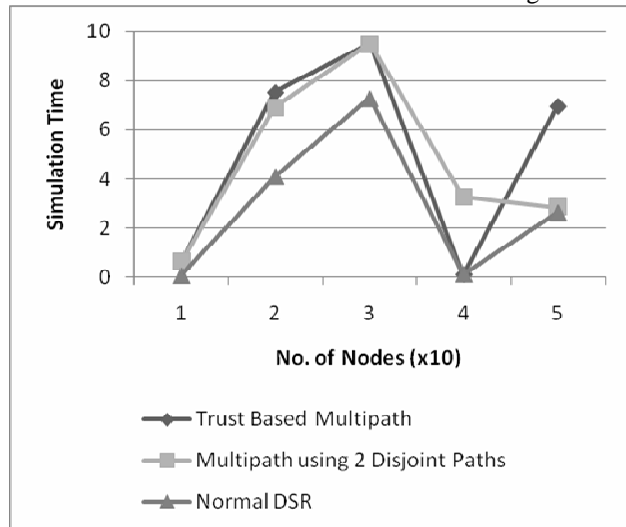


Figure 6: Route Selection Time

are presented in Figure 6. Since DSR selects the first path it receives as the path set, the route selection time of DSR is minimum. The disjoint multipath routing algorithm has to wait for at least 2 paths till it can select a path set. In addition, it may have to wait for a longer time depending on how much time it takes to receive a disjoint path. A node may not receive a disjoint path at all, in case a 'vital' node

exists or if there is not enough redundancy in the network. Trust based multipath routing generally (but not always) takes the longest time in route selection since it requires trusted paths which may take a longer time coming. But in cases where all the nodes of the path received first are trusted, the route selection time of trust based multipath routing can be equal to that of a normal DSR. The route selection times of all three algorithms depend on the placement of source and destination nodes in a network and also on the network topology.

Hence, we observe that there is a compromise between message security (trust compromise) and routing time (route selection time), which is generally the case with most of the security algorithms. A balance must be struck between the two parameters to provide maximum security without causing substantial delay for a user.

## 6. CONCLUSION

We presented a trust based multipath algorithm for message security in mobile ad-hoc networks. We first proposed a *trust defined strategy* for route set selection and then implemented it using DSR. We simulated the algorithm and compared the results with the following traditional algorithms: normal DSR and multipath routing using disjoint path. It was found that the proposed algorithm is much more secure than both normal DSR and multipath routing using disjoint paths but it generally takes more time in route selection in comparison.

## REFERENCES

- [1] Haniotakis, T. Tragoudas, S. and Kalapodas, C., "Security enhancement through multiple path transmission in ad hoc networks," *IEEE International Conference on Communications, 2004*, vol.7, no., pp. 4187-4191 Vol.7, 20-24 June 2004
- [2] Abdul-Rahman, A. and Hailes, S. 1997. "A distributed trust model", *In Proceedings of the 1997 Workshop on New Security Paradigms* (Langdale, Cumbria, United Kingdom, September 23 - 26, 1997). NSPW '97. ACM Press, New York, NY, 48-60.
- [3] Pirzada, A.A.; Datta, A.; McDonald, C., "Propagating trust in ad-hoc networks for reliable routing," *2004 International Workshop on Wireless Ad-Hoc Networks*, vol., no., pp. 58-62, 31 May-3 June 2004
- [4] Pirzada, A. A. and McDonald, C. 2004. "Establishing trust in pure ad-hoc networks", *In Proceedings of the 27th Australasian Conference on Computer Science - Volume 26* (Dunedin, New Zealand). Estivill-Castro, Ed. ACM International Conference Proceeding Series, vol. 56. Australian Computer Society, Darlinghurst, Australia, 47-54
- [5] Buttyan, L., and Hubaux, J.-P. "Stimulating Cooperation in Self-Organizing" *Journal Article on Mobile Networks and Applications*, Springer Netherlands, pp. 579-592, Volume 8, October, 2004
- [6] Buchegger, S. and Le Boudec., J. Y., "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes --- Fairness In Dynamic Ad-hoc NeTworks". *In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Lausanne, CH, June 2002.
- [7] Michiardi, P. and Molva, R. 2002. "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks". *In Proceedings of the IFIP Tc6/Tc11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security* (September 26 - 27, 2002). B. Jerman-Blazic and T. Klobucar, Eds. IFIP Conference Proceedings, vol. 228. Kluwer B.V., Deventer, The Netherlands, 107-121.
- [8] Hu, Y-C, Perrig A., and Johnson, D., B. "Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks," in *Journal Article on Wireless Networks*, Springer Netherlands, pp. 21-38, Volume 11, February 2005
- [9] Papadimitratos, P. and Haas, Z. J. 2003. Secure data transmission in mobile ad hoc networks. *In Proceedings of the 2003 ACM Workshop on Wireless Security* (San Diego, CA, USA, September 19 - 19, 2003). WiSe '03. ACM Press, New York
- [10] Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., and Belding-Royer, E. M. 2002. A Secure Routing Protocol for Ad Hoc Networks. *In Proceedings of the 10th IEEE international Conference on Network Protocols* (November 12 - 15, 2002). ICNP. IEEE Computer Society, Washington, DC, 78-89.
- [11] Cidon, I., Rom, R., and Shavitt, Y. 1999. "Analysis of multi-path routing", *IEEE/ACM Trans. Netw.* 7, 6 (Dec. 1999), 885-896
- [12] Lou, W., Liu, W., Fang, Y., "SPREAD: enhancing data confidentiality in mobile ad hoc networks," *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, vol.4, no., pp. 2404-2413 vol.4, 7-11 March 2004
- [13] Mishra, A., Nadkarni, K., M., "Security in Wireless Ad-Hoc Networks. Chapter 30, *The Handbook of Wireless Ad-Hoc Networks*, edited by Ilyas, M., CRC Press, ISBN 0849313325, 2003.
- [14] Johnson, D., B., Maltz, D., A., and Broch, J., "DSR The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks", *In Ad Hoc*

- Networking*, edited by Charles E. Perkins, chapter 5, pages 139--172. Addison-Wesley, 2001
- [15] Wang, W., Zhu, Y., Li, B., "Self-managed heterogeneous certification in mobile ad hoc networks", *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, vol.3, no., pp. 2137-2141 Vol.3, 6-9 Oct. 2003
- [16] Pirzada, A.A.; Datta, A.; McDonald, C., "Trust-based routing for ad-hoc wireless networks," *Networks, 2004. (ICON 2004). Proceedings. 12th IEEE International Conference on*, vol.1, no., pp. 326-330 vol.1, 16-19 Nov. 2004
- [17] Takai M., Bajaj, L., Ahuja, R., Bargrodia, R., and Gerla, M., "GloMoSim: A Scalable Network Simulation Environment", *Technical report 990027*, UCLA, Computer Science Department, 1999.
- [18] R. Bargodia, R. Meyer, M. Takai, Y. Chen, X. Zeng, J. Martin and H. Y. Song, "PARSEC: A Parallel Simulation Environment for Complex Systems", *IEEE Computers*, Vol. 31, No. 10, Oct. 1998, pp 77-85.
- [19] IEEE Computer Society LAN MAN Standards Committee, Wireless LAN Medium Access Protocol (MAC) and Physical Layer (PHY), IEEE Std. 802.11 -1997. The Institute of Electrical and Electronic Engineers, 1997.