Journal of Theoretical and Applied Information Technology
31st August 2013. Vol. 54 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURE ZONE BASED ROUTING FOR BLUETOOTH SCATTERNETS

[1]SARAH MARYIUM,[2]SAMAN ZEHRA, [3]MALIK SIKANDER HAYAT KHIYAL,[4]M. SHERAZ BAIG
[1,2]Department of Computer Science, International Islamic University, Islamabad.
[3]Professor and Head of Academic, Army Public College of Management and Sciences, Khadim Hussain Road, Lalkurti, Rawalpindi.
[4]Management Information System, Army Welfare Trust, The Mall, Rawalpindi
E-mail: [3]m.sikandarhayat@yahoo.com, [4]shiraz_baig@yahoo.com

ABSTRACT
Bluetooth (BT) is presently the primary wireless technology for short range Personal Area Network (PAN). Piconet is the basic unit of networking in BT that contains one master and from one to seven active slave devices. Piconets can be interconnected to form a scatternet. Scatternet formation and routing are the important areas on which considerable research has been done so far. Security is another important issue for BT scatternets. BT specification provides security measures for piconets but secure communication in a scatternet is an open problem. In our research we specifically consider routing security in BT scatternets. We describe a number of routing threats and then present an authenticated routing scheme which is based on Zone Routing Protocol. We evaluate the scheme through simulation and show that it effectively secures the route discovery process in BT scatternets.
Keywords: — *Bluetooth, Personal Area Networks, Piconet, Scatternet, Zone Routing Protocol, Routing Attack.*

1. INTRODUCTION

Bluetooth [1] is an open standard specification for a radio frequency (RF)-based short-range connectivity technology that promises to change the face of computing and wireless communication. It is designed to be an inexpensive, wireless networking system for all classes of portable devices, such as Laptops, PDA's (Personal digital assistants), and mobile phones. It also will enable wireless connections for desktop computers, making cable-free connections between monitors, printers, keyboards, and the CPU. The Bluetooth specification, while innovative, does not define a totally new technology. In fact, Bluetooth draws heavily on existing radio communications and networking technologies, which enables it to be operationally compatible with the existing devices that also use these technologies. Many of the various terms and concepts used in Bluetooth are borrowed from other areas and included in the specification of Bluetooth's elements, such as base band, RF communication, and many of the upper- and lower-layer protocols.

The major difference between Bluetooth wireless connectivity and the cellular radio architecture is that Bluetooth enables ad hoc networking. Rather than depending on a broadband system, which relies on terminals and base station for maintaining connections to the network via radio links, Bluetooth implements peer to peer connectivity- no base station or terminals are involved.

Bluetooth has two physical topologies piconet and scatternet. Bluetooth protocols assure that a small number of units will participate in communications at any given time. These small groups are called piconets and they consist of one master unit and up to seven active slave units. If several piconets overlap a physical area, and members of the various piconents communicate with each other, this new, larger network is known as a scatternet.

According to [2] the major requirements of a routing protocol are: (i) minimum route acquisition delay, (ii) quick route reconfiguration in the case of path breaks, (iii) loop-free routing, (iv) distributed routing protocol, (v) low control overhead, (vi) scalability with network size, (vii) Qos support as demanded by the application, (viii) support of time sensitive traffic, (ix) security and privacy. Based on the routing information update mechanism, routing protocols in ad hoc wireless networks can be

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

classified as proactive (or table-driven) protocols, reactive (or on-demand) protocols and hybrid routing protocols. In proactive routing protocols, nodes exchange routing information periodically in order to maintain consistent and accurate routing information for example, Destination Sequence Distance Vector (DSDV), Wireless Routing Protocol (WRP), Optimized Links State Routing (OLSR), etc. In the reactive routing protocol, a route discovery mechanism is initiated only when a node does not know a path to a destination it wants to communicate with. Ad hoc On-Demand Vector (AODV), Dynamic Source Routing (DSR), Temporally Ordered Routing Algorithm (TORA) are examples of reactive routing protocols. Some ad hoc network routing protocols are hybrid of proactive and reactive mechanisms. Examples of hybrid routing protocols are Zone Routing Protocol (ZRP), Core Extraction Distributed Ad hoc Routing protocol (CEDAR), etc.

[3] discussed a hybrid scheme, the Zone routing Protocol (ZRP) that combine the advantages of both proactive and reactive approaches, taking advantage of

proactive discovery within a node's local neighborhood, and using a reactive protocol for communication between these neighborhoods. In order to assure a reliable data transfer over the communication networks and to protect the system resources, a number of security services are required. Based on their objectives, the security services are classified in five categories [4]: availability, confidentiality, authentication, integrity and non-repudiation. The majority of traditional routing protocols design fails to provide security. According to [2] the main requirements of secure routing protocols are: i) detection of malicious nodes, ii) guarantee of correct route discovery, iii) confidentiality of network topology, and iv) stability against attacks.

Providing a secure system can be achieved by preventing attacks or by detecting them and providing a mechanism to recover for those attacks. Attacks on Ad Hoc wireless networks can be classified an active and passive attack, depending on whether the normal operation of the network is disrupted or not. Active attacks can be further divided into internal and external attacks.

2. RELATED WORK

According to [5] mobile Ad Hoc networks have inherently different properties than traditional wired networks. These new characteristic present different security vulnerabilities and provide a detailed classification of these threats.

[6] focuses on the gap between proposed Ad Hoc routing protocols and the means to make them secure. According to [7] the existing wireless routing protocols do not accommodate any security and are highly vulnerable to attacks.

Three types of potential vulnerabilities in the Bluetooth standard version 1.0B is pointed [8]. The first vulnerability opens up the system to an attack in which adversary under certain circumstances is able to determine the key exchanges between two victim devices, making eavesdropping and impersonation possible. Second vulnerability makes possible a location attack in which attacker is able to determine the geographic location of the victim device. The third vulnerability concerns the cipher.

The replay attacks on Bluetooth authentication protocol is describe in [9]. The aim of these attacks is impersonation.

A routing strategy for Bluetooth scatternets is proposed in [10]. A concept of hierarchical scatternet has been proposed that is adapted for large amount of devices connected along each other with a predefined routing strategy. All piconets are coordinated according to a free structure and are perfectly synchronized to a leader.

A routing scheme for Bluetooth scatternets presented in [11] which is based on the Zone Routing Protocol. The routing scheme is designed keeping in mind the specifics of the Bluetooth technology. The scheme gives very low overhead while keeping the route acquisition latencies low. The routing information at a node does not require a large amount of storage.

Secure Efficient Ad Hoc Distance Vector (SEAD) [12] is designed which is a proactive routing protocol based on the design of DSDV [13]. Besides the fields common with DSDV, such as destination, metric, next hop and sequences number, SEAD routing tables maintain has a value for each entry.

Another protocol ARIADNE [14] designed, an efficient on demand secure routing protocol, provides security against arbitrary active attacks and relies only on efficient symmetric cryptography. It prevents attacks from tampering uncompromised routes consisting of uncompromised nodes. However, for secure authentication of a routing message, it relies on the TESLA [15] broad cast authentication protocols.

Security Aware Routing (SAR) [16] is an on demand routing protocol based on AODV. It integrates the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

trust level of a node and the security attributes of a route to provide an integrated security metric for the requested route.

Secure Routing Protocol (SRP) [17] is another protocol extension that can be applied to many of the on demand routing protocols. SRP defends against attacks that disrupt the route discovery process and guarantees to identify the current topological information. The basic idea of SRP is to set up a security association (SA) between a source and a destination node without the need of cryptographic validation of the communication data by the intermediate nodes.

A secure routing protocol for ad hoc networks (ARAN) [18] is an on-demand protocol designed to provide secure communication in managed open environments, Cooperation of Nodes Fairness. In Dynamic Ad hoc NeTworks (CONFIDANT) [19] protocol is designed as an extension to reactive source routing protocol such as DSR. It is collection of components which interact with each other for monitoring, reporting, and establishing routes by avoiding misbehaving nodes.

3. RESEARCH METHODOLOGY

A large number of attacks have been identified in literature that effects the routing in ad hoc wireless networks and so the routing in Bluetooth based MANET's. These routing attacks can be classified into five categories: attacks using impersonation, modification, fabrication, and replay. Attacks using impersonation are man-in-the-middle attack, spoofing, Sybil attack etc. Attacks using modification are misrouting attack, blackmail attack etc. Attacks using fabrication are resource consumption attack, routing table poisoning, rushing attack, black hole, Gray Hole etc. Replay attacks are worm hole attack, tunneling attack etc.

A number of security solutions for ad hoc wireless protocols (either proactive or reactive) have been proposed, but none of them provides a hybrid security solution. Also direct application of these security solutions may be inefficient for Bluetooth scatternets. As Zone Routing Protocol (ZRP) combines the advantages of both the proactive and reactive approaches; we provided a hybrid security solution that secured both the table driven as well as on-demand routing, and this is achieved through authentication. We designed a secure routing scheme based on ZRP keeping in mind the specification of Bluetooth.

The security against most of the above mentioned attacks can be achieved through authentication. Not only does it matters to keep the information safe from eavesdroppers or otherwise unauthorized readers. The need for knowing that the sender actually is the sender is important for secure systems. In some cases this need is even more important than the one of confidentiality. It might be of more importance to know that a certain message actually is from the one who it says it is than to keep the information it holds secret.

Authentication information will comprise of a signature, which will be calculated by the combination of the key, unique identification number of each node and the time stamp. The key is generated by the public-private key pair, key message and the key-generation algorithm.

The main modules of our system can be viewed as follows:

- Node Registration Phase: The nodes, at the beginning are required to be assigned properly. In this phase each node will be assigned a pair of public-private key pair and unique identification number. Then there is an exchange of public key between Certificate Authority (CA) and the node, to make that public key available to all nodes. In turn, the Certificate Authority having the list of public keys with unique identification numbers issues a certificate. As a result of this process, Certificate Authority (CA) has public keys of all the nodes that are to enter in the network. After this process, all the un-trusted nodes will be converted into trusted nodes.
- Authentication & Verification Phase: The Certificate Authority (CA) periodically distributes certificate containing the list of public keys with corresponding unique identification number of all the nodes.
  - ➢ Authenticated Neighbor Discovery: A node accepts signed control messages (HELLO messages) from trusted neighborhood.
  - ➢ Authenticated Route Discovery: If a node wants to send a packet to another node in the network, it computes the signature using its private key and sends it to the destination node. To authenticate the sending node, the destination node

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

acquires the public key of sending node from the certificate and computes the signature itself. Also all the relay nodes authenticate each other through the same process. If both the signatures match, the signature is validated and sending/relaying node is proved to be an authenticated node.

- Dealing with malicious nodes: this involves detecting malicious nodes and reacting to them.

According to [18] all secure ad hoc protocols must satisfy the following requirement to ensure that path discovery from source to destination functions correctly in the presence of malicious adversaries: i) route signaling cannot be spoofed, ii) fabricated routing messages cannot be injected into the network, iii) routing messages cannot be altered in transit, except according to the normal functionality of the routing protocol, iv) routing loops cannot be formed through malicious action, v) routes cannot be redirected from the shortest path by malicious action, vi) unauthorized nodes must be excluded from route computation and discovery, vii) the network topology must neither be exposed to adversaries nor to the authorized nodes by the routing messages

4. FUNDAMENTALS OF THE PROTOCOLS

A. Node Registration/Certification:

Our protocol use Cryptographic Certificates [18] to bring authentication, message integrity and non-repudiation to the route discovery process. It therefore requires the use of a trusted certificate authority T, whose public key is known to all nodes (or multiple servers may be used [20]). Nodes use these certificates to authenticate themselves to other nodes during the exchange of routing messages.

Before entering the scatternet, each node must request a certificate from certificate authority (CA) or T. each node receives exactly one certificate after security authenticating its identity to T. For example node A receives a certificate from T as the formula given by [18].

T_A: $cert_A = [BD\_ADDR_A, KU_A, t, e]KR_A$

Where,

KU_A: Public key of node A

KR_A: Private key of node A

$cert_A$: certificate belonging to A

t: time stamp

e: certificate expiring time

BD_ADDR_A: Bluetooth address of a node A.

The certificate contains the Bluetooth address BD_ADDR, address of the device ([18] uses IP address of A), its public key, a time stamp of when the certificate was created, and expiry time of the certificate.

B. Authentication and verification Phase:

1. Authenticated Neighbor Discovery:

The proactive neighbor discovery module allows nodes to discover who is in their _-hop neighborhood where, _ is the radius of the zone. This is achieved by all nodes advertising their 1-hop neighborhoods to each other. This part of the protocol is proactive; as such node has to periodically broadcast updates indicating any changes to their 1-hop neighborhood. A node accepts signed HELLO messages from trusted neighborhood and how it verifies them will be explained next.

Only master or gateway node maintain a routing table which contains an entry for each master node from which it has received a Hello message and a list of the addresses of that master nodes immediate neighbors.

2. Authenticated Route Discovery:

The second phase is the reactive route discovery used to discover new routes when they are needed. If a node requires a route to a destination which is not within the nodes _-hop neighborhood, it broadcasts a route request message, which contains the addresses of both the originating node and the destination node.

As [18] uses the command to broadcasting route discovery packet (RDP) of source node to destination node; we similarly use to broadcast the route request packet (RREQ) from source node A to destination node X.

A _broadcast:$[RREQ, BD\_ADDR_X] KR_A, Cert_A$

Let B be a neighbor that has received from A the RREQ broadcast, which it subsequently rebroadcasts as used by [18].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

B_broadcast:[[RREQ, BD_ADDR_X] KR_A] KR_B, $Cert_A$, $Cert_B$

3. Authenticated Route Setup:

After receiving the RREQ, the destination unicasts a route reply (RREP) packet back along the reverse path to the source. Let the first node that receives the REP sent by X be node D, as used by Sanzgiri et al. [2002].

X _ D: [RREP, BD_ADDR_A]KR_X, $Cert_X$

Let D's next hop to the source is node C then the command is as used by Sanzgiri et al. [2002].

D _ C: [[RREP, BD_ADDR_A]KR_X]KR_P, $Cert_X$, $Cert_D$

C validates D's signature on the received message, removes the signature and certificate, then signs the contents of the message and appends its own certificate before unicasting the RREP to B, as used by [18].

C _ B: [[RREP, BD_ADDR_A]KR_X]KR_C, $Cert_X$, $Cert_C$

C. Dealing with Erratic Behavior:

When no traffic has occurred on an existing route for that route's lifetime, the route is simply deactivated in the route table. Data received on an inactive route causes nodes to generate an error (ERR) message. Nodes also use ERR messages to report links in active routes that are broken due to node movement. All ERR messages must be signed.

5. RESULTS

We evaluate the performance of S-ZRP using measurements obtained through both simulation and implementation. Simulation enables us to measure the effectiveness and efficiency of S-ZRP in reasonably large networks, with and without the presence of malicious nodes. Although simulation is a useful tool for anticipating protocol performance in real networks, it needs to be complemented with protocol implementation in order to obtain a more realistic evaluation of the protocol.

It is to be noted that the energy cost of cryptographic operations could be of some concerns, particularly in resource-constrained mobile devices. However, the energy consumed by wireless communication is significantly higher; additionally, route discovery is performed infrequently in most ad hoc networks. We, therefore, do not consider the energy consumption of cryptographic computations to be significant, and do not measure it in our experiments.

We have conducted two types of test to determine the overhead of using certificates and signatures in ZRP. These tests include measurements of raw processing time per routing packet for different number of nodes, and measurements of the average route acquisition latency.

1. Message Processing Time: We examined the raw processing time expended at a node for a ZRP packet. Specifically, we measured the processing time required for a node to receive a packet from a neighbor that is not the initial sender of the packet, verify that the neighbor's signature on the message, strip off the neighbor's certificate, add its own certificate, sign the message, and then rebroadcast the message. Measuring per node processing time on this type of packet gives us an upper bound on the processing time for a routing message at each node. Hello messages and error messages require less processing time. We conducted this test by mirroring the sequence of function calls that are performed when a packet is received by S-ZRP.
2. Route Acquisition Latency: We also measured the average route acquisition latency, which is the delay from route request initiation to the receipt of a corresponding reply. The results of measuring latency in this way depend on the number and topology of network nodes.

6. COMPARISON OF ZRP AND S-ZRP

Average Route Acquisition Latency: This is the average delay between the sending of a route request/discovery packet by a source for discovering a route to a destination and the receipt of the first corresponding route reply. If a route request timed out and needed to be retransmitted, the sending time of the first transmission was used for calculating the latency.

Journal of Theoretical and Applied Information Technology
31st August 2013. Vol. 54 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

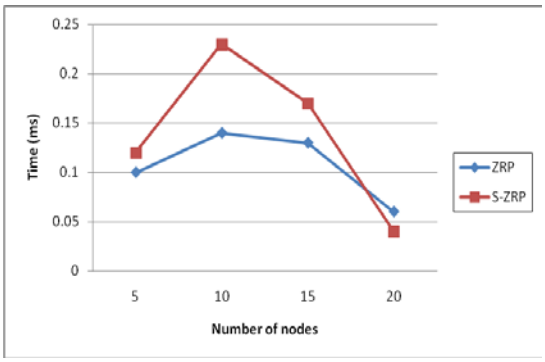

Fig. 1. Simulation Results- Average Route Acquisition Latency

Figure 1 shows that malicious nodes can exploit ZRP so that no-shortest paths are selected, while such exploitation is not possible with S-ZRP. This metric indicates the extent of path elongation in ZRP is because of the presence of different malicious nodes, which cannot be detected.

Average Processing Time at each node: This is the time taken for a packet on a single node i.e. the time in which node verifies the sender and appends its own signature.

Figure 2 show that the average route acquisition latency for S-ZRP is slightly higher than that of ZRP. While processing S-ZRP control packets, each node has to verify the digital signature of the previous node, and then replace this signature with its own digital signature, in addition to the normal processing of the packet as done by ZRP. The cryptographic operations cause additional delays at each hop, and so the route acquisition latency increases.

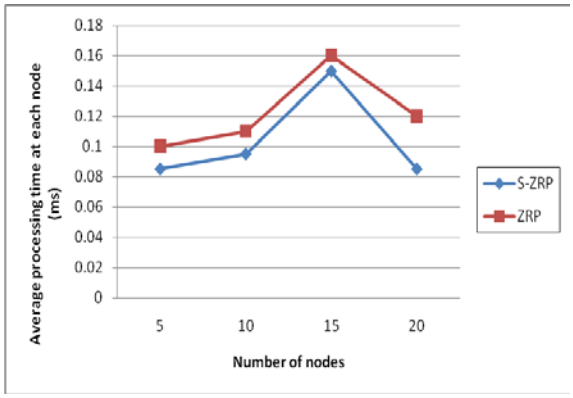

Fig. 2. Simulation Results- Average Processing Time at each node

Fraction of data packets dropped that passed through malicious nodes: This metric indicates the fraction of data packets that traverse malicious nodes when using each routing protocol, in the presence of different percentages of malicious nodes. The metric is important because data packets passing through malicious nodes are overheard by these nodes, and could potentially be modified or dropped.

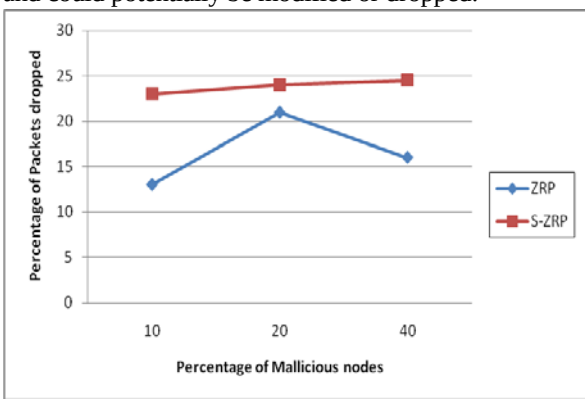

Fig. 3. Simulation Results- Percentage of Packets Dropped

Figure 3 show that when using ZRP, a much larger fraction of data packets passes through malicious nodes, as compared with using S-ZRP. For instance, in the presence of 10% malicious nodes with no node mobility, 23% of data packets drop through malicious nodes when using S-ZRP, as compared with almost 13% when using ZRP. This is because malicious nodes can potentially manipulate ZRP to make routes pass through themselves.

7. CONCLUSION

Popular ad hoc routing protocols are subject to a variety of attacks, which, through modification or fabrication of routing messages or impersonation of other nodes, can allow attackers to influence a victim's selection of routes or enable denial-of-service attacks.

Our proposed architecture S-ZRP, provides secure routing or the managed-open and open environment. S-ZRP provides authentication and non-repudiation services using cryptographic certificates that guarantees end-to-end authentication. In doing so, S-ZRP limits or prevents attacks that can affect other insecure protocols. Summarizing through the above results, it could be said that

- S-ZRP is a simple architecture that does require some additional processing from each node
- S-ZRP is as effective as ZRP in discovering and maintaining routes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- S-ZRP detects false packets and packets from malicious nodes in a far better manner than in case of ZRP
- S-ZRP drops wrong packets more effectively as compared to original ZRP.

The impact of the overhead caused would be almost insignificant and negligible as compared to the proposed degree of security, which S-ZRP will provide to any network system if adopted in letter and spirit.

REFERENCES:

[1] "specification of the Bluetooth system". Version v2.0, volumes 0-3, available at http://www.bluetooth.org, November 2004.

[2] C.S.R. Murthy and B.S. Manoj. Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, 2004.

[3] Z.J. Haas, M.R. Pearlman, P. Samar. "The Zone Routing Protocol (ZRP) for Ad Hoc Networks". IETF Internet Draft, draft-ietf-manet-zone-zrp-04, July 2002.

[4] W. Stallings. Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall. 2003.

[5] P_W Yau and C. J. Mitchell. "Security vulnerabilities in Ad Hoc Networks". In the seventh International symposium on communication theory and application, July 13-18, 2003, Ambleside, Lake District, UK, pages 99-104, HW communication Ltd.

[6] C. Gahlin. Secure Ad Hoc Networking. Master Thesis in Computer Science, Department of Computing Science at Umeå University, 1st March 2004. cs.umu.se/education/examina/Ra...

[7] Qifeng Lu. "Vulenrability of Wireless Routing Protocols", University of Massachusetts, Amherst, Dec 15, 2002.

[8] M. Jacobson and S. Wetzel. "Security weaknesses in Bluetooth". In CT-RSA 101, LNCS 2020, Springer Verlog 2001, pp 176-191.

[9] E. Cetintas, M. Aydos, C.K. Koc and M.U. Caglayan. "Relay attacks on Bluetooth authentication and solutions". In *ISCIS 2004* - The 19th International Symposium on Computer and Information Sciences, Antalya, Turkey, Springer-Verlag, LNCS 3280, pp. 278 - 289, October 2004.

[10] C. Lafon and S.T. Durrani. "Bluetooth throughput improvement using a slave to slave piconet formation". HSNMC 2003: 254-263.

[11] R. Kapoor and M. Geral. "A Zone routing protocol for Bluetooth scatternets, wireless communications and networking conference", WCNC 2003, March 2003, New Orleans, Louisiana.

[12] Y.-C. Hu, D.B. Johnson and A. Perrig. "SEAD: secure efficient distance vector routing for mobile wireless Ad Hoc Networks", fourth IEEE workshop on mobile computing systems and applications (WM-CSA'02), June 2002.

[13] C.E. Perkins and P. Bhagwat. "Highly dynamic destination-sequences distance vector routing (DSDV) for mobile computers", SIGCOMM'94 conf. on communications architectures, protocols and applications, Aug. 1994, pp. 234-244.

[14] Y.-C. Hu, A. Perrig and D.B. Johnson. "Ariadne: A secure on-demand routing protocol for Ad. Hoc Networks", In *Proc* of the Eighth Annual International Conference on Mobile Computing and Networking (ACM Mobicom'02), Atlanta, Georgia, September 23 - 28, 2002.

[15] A. Perrig, R. Canetti, D. Song and D. Tygar.. "The TESLA broadcast authentication protocol", RSA cryptobytes (RSA Laboratories), vol 5, no 2, Summer/Fall 2002, pp. 2

[16] S. Yi, , P. Naldurg and R. Kravets." A security-aware routing protocol for wireless Ad Hoc Networks". The 6th World Multi-Conference on Systemic, Cybernetics and Informatics (SCI 2002).

[17] P. Papadimitriou and Z.J. Haas. "Secure routing for mobile Ad Hoc networks", in *proc*. Of the SCS communication networks and distributed systems modeling and simulation conference (CNDS 2002), Jan. 2002.

[18] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M.B. Royer. "A secure routing protocol for Ad Hoc networks", the 10th IEEE Intl. conf. on network protocol (ICNP), Nov. 2002.

[19] S.Buchegger and J.-Y. Le. Boudec. "Performance analysis of the CONFIDANT protocol cooperation of nodes fairness in dynamic ad hoc networks", in *proc*. Of IEEE/ACM symposium on mobile ad hoc networking and computing (MobiHOC), June 2002, pp 226-236.

[20] L. Zhou and Z.J. Haas. "Securing Ad Hoc networks", IEEE network, Vol 13, no. 6, pp. 24-30, 1999.