Trusting the Trust-Model in mobile wireless ad-hoc network settings

DAGMARA SPIEWAK, THOMAS ENGEL
University of Luxembourg
Faculty of Sciences, Technology, and Communication
6, r. Richard Coudenhove-Kalergi, L-1359 Luxembourg
LUXEMBOURG

Abstract: - Nowadays, the world gets more and more mobile in such a way that communication services are desirable anytime and anywhere. In this context, *Mobile wireless ad-hoc networks*, including mobile ad-hoc networks (*MANETs*) and *Mesh-Networks*, are systems of nodes that interconnect in a dynamical self-organized way providing an attraction especially during mission-crucial or time-crucial applications, for example during a disaster recovery scenario, allowing to extend common Wireless LAN technologies over wide areas. However, the nature of mobile wireless networks makes them very vulnerable to malicious attacks and selfish actions. Principally, due to the absence of pre-established communication infrastructure, *security* in *mobile ad-hoc wireless networks* is assumed trickier than in conventional and hierarchical network systems. Unfortunately, traditional and approved security mechanisms are not applicable in such almost anarchistic network structures. Thus, the establishment of *Trust* is virtually ubiquitous and could lead to a milestone regarding security in *mobile wireless ad-hoc networks*. In this paper, we compare *Trust* evaluation, *Trust* evidence and *Trust* evidence distribution approaches concerning their applicability to mobile wireless network settings with the aim to figure out which model is truly trustworthy.

Key-Words: - Mobile wireless ad-hoc networks, Trust, Security, Attacks, MANET, Mesh-Networks

1 Introduction

Crucial data and applications transmitted within mobile wireless networks require a high degree of security. Principally, due to the absence of fixed base stations and pre-established infrastructure, these networks differ highly from traditional hierarchical networks. MANETs for instance, allow nodes to form and leave the network dynamically, sometimes even without leaving a trace. Even though, accepted securing techniques, like common public-key encryption and digital signatures are not accurate, it is understandably very important to provide security services such as authentication, confidentiality, and privacy, if required. As a consequence, recent research topics concentrate on *Trust-Metrics* for the purpose of overcoming the weakness of having a continuously accessible and central Trusted Third Party *(TTP)* managing the network's security and simultaneously representing a dangerous bottleneck of the system. Although *Trust* is well known to everybody, the formal definition poses several challenges. The papers [1] and [2] present a wide expertise on the description of *Trust* as well as its relationship regarding *Security*. In [3] the notion of *Trust* in mobile wireless ad-hoc network settings is directly compared to *Trust* applied to the Internet, for instance while thinking of the *PayPal* Payment System, and the necessity of the autonomy of pre-established *Trust* infrastructures is highlighted. Additionally, the interdependency of *Trust* and *Security* is emphasized in [4], concluding that security is highly dependent on trusted key exchange. However, trusted key exchange on the other side can only take place with requisite security services.

The contribution of this paper is to present different *Trust* establishment methods and to analyze their application to mobile wireless ad-hoc network settings. Section 2 illustrates possible security attacks in mobile wireless ad-hoc networks before Section 3 subsequently summarizes relevant *Trust Models*. Finally Section 4 concludes the paper.

2 Attack Analysis

Generally, two kinds of security attacks can be launched against mobile wireless ad-hoc networks, *passive* and *active* attacks. The adversary rests unnoticed in the background while running a *passive* attack, even without disturbing the functions of the protocol, and eavesdrops worthwhile information about the networks and the participating network entities. While launching *active* attacks, the attacker disturbs the correct functionality of the routing protocol by for instance modifying routing information or running Denial of Service attacks. Buchegger and Boudec [5] underline the importance of *Trust* in order to isolate malicious nodes and to establish reputation systems in all nodes that enable them to detect misbehavior of network participants.

In the following, categories of *active* attacks associated with vulnerabilities of mobile ad-hoc systems are listed.

2.1 Integrity Attacks

By launching an *Integrity Attack* the malicious node drops messages, redirects traffic to a different destination, or computes longer routes in order to increase the communication delays. The most famous attack in this category is the set-up of a *Blackhole* [6] where the attacker swallows all packets traversing its node. As an extension the active attacker might launch a *Greyhole* [7] attack allowing him to switch its cause of action from forwarding packets and discarding others. Even trickier is the establishment of a tunnel in the network between two or more cooperating and by the attacker compromised nodes that are linked through a private network connection, called *Wormhole* [8] allowing the attacker to short-cut the normal flow of packets. After *tunneling* the packets to another point in the mobile wireless ad-hoc network, the attacker replays them into the network. These three attacks can also be grouped as *Byzantine Attacks* discussed in [9]. The following figure shows the classification of attacks in mobile wireless ad-hoc networks.

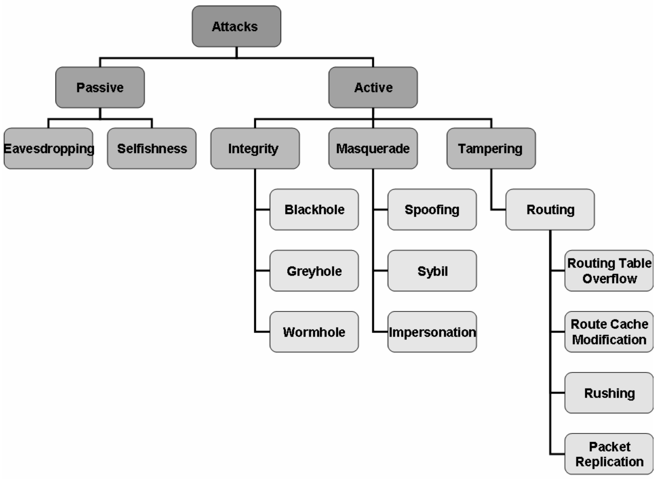

Fig.1 *Classification of Attacks in mobile wireless ad-hoc networks*

2.2 Masquerade Attacks

These types of attacks are often known as *Spoofing Attacks*, where the attacker modifies either the MAC or the IP address in outgoing packets with the aim to adopt another identity in the network and appear as a good-natured node. By this technique, he may operate as a trustworthy node and may for instance advertise incorrect routing information. Another dangerous attack is known as *Sybil Attack* [10] where the malicious node may not only impersonates one other node but multiple false identities. Particularly mobile networks that apply a Recommendation-Based *Trust-Model* are vulnerable to *Sybil Attacks*. Here the malicious node can generate fake recommendations about the trustworthiness of a particular node in order to attract more network traffic to it offering an ideal starting point for *Wormhole Attacks*.

2.3 Tampering Attacks

These attacks are based on the distribution of falsified routing messages and are difficult to identify and trace. The *Rushing Attack* [11] is one example for such an attack acting as an effective Denial of Service attack against all currently proposed on-demand ad-hoc network routing protocols. Launching this attack the adversary rapidly spreads routing messages all through the network, disabling authorized routing messages with the consequence, that other nodes delete them as multiple copies. Obviously, also computational routes towards a destination can be canceled by constructing routing error messages and consequently asserting that the neighbor can not be reached. So, since flooding is the famous mechanism used by on-demand routing protocols in order to establish paths, disturbing the flooding procedure is an effective attack against this category of protocols.

3 Trust Models

The establishment of *Trust* as the foundation for succeeding security principles, like for instance authentication, resounds throughout the land. However, many solutions misleadingly introduce *Trust* as a matter of course by simultaneously using it as the basis for further security issues, without even constructing a conclusive *Trust Metric*. As in [12] clarified, "*Trust is interpreted as a relation among entities that participate in various protocols*". Consequently, the trustworthiness of a certain entity depends also on its former behavior within the protocol.

In the following, we discuss several *Trust Models* with the objective of answering the question: *"Which Trust Model is trustworthy and reliable in mobile wireless network settings?"*

3.1 PGP Trust Model

Pretty Good Privacy or *PGP* [13], is an important milestone in the history of cryptography, because for the first time cryptography is available to a wide community. It was principally created for encrypting or signing email messages and offers a hybrid cryptosystem. The basic idea is that all users operate as autonomous certification authorities giving them the right to sign and verify keys of other entities. The absence of a central certification authority and the introduction of the so-called *Web of Trust* allow network entities to build a set of virtual interconnections of *Trust*.

However, can we *trust PGP* in mobile wireless ad-hoc network settings as well? After an explicit evaluation of the model, we must negate this question. Although no central authority is required to sign the public-keys, the distribution of these keys is managed by a continuously accessible public-key directory that resides on a centrally managed server making *PGP* inadequate in mobile ad-hoc network settings where nodes may join and leave the network spontaneously.

3.1.1 Adjusting PGP to mobile wireless ad-hoc network settings

In [14] *PGP* is extended by a public-key distribution system that fits better to the self-organized nature of mobile wireless ad-hoc networks. Similar to *PGP*, public-key certificates are issued, signed and verified by nodes in the network themselves. Additionally, each node maintains a *local certificate repository* that contains a subset of public-keys of network's entities. As a consequence, nodes may manage the distribution of public-key certificates by themselves as well. However, the establishment as well as the update procedure of the *local certificate repository* is a computationally complex operation producing an extensive overhead while executed on resource constrained devices, like for instance PDAs. Moreover, the detailed analysis of the utilized algorithm demonstrates the high vulnerability to *Sybil Attacks* of the adjusted *PGP* model. Finally we conclude that the weaknesses in security paired with the high computational complexity make this *Trust Model* impractical for mobile wireless ad-hoc network settings.

3.2 Decentralized Trust Model

The *Decentralized Trust Model* [15] was the foremost system creating a comprehensive model of *Trust*, which is independent of any particular application or service. It extends the common identity-based certificates, which bind a public-key to a unique identity, by means of reliably mapping identities to actions they are trusted to perform. The main achievement was the construction of a system called *PolicyMaker* in order to define policies and *Trust* relationship composed with the *PolicyMaker Language*. While this approach provides a basis for expressing and evaluating *Trust*, it does not consider the simultaneous problem of how to continuously control and manage *Trust* over a longer period of time, which is discussed in [16].

3.3 Distributed Trust Model

The *Distributed Trust Model* [17] applies a recommendation protocol to exchange, revoke and refresh recommendations about other network entities. Therefore, each entity needs its own *Trust Database* to store different categories of *Trust* values ranging form -1 (complete distrust) to 4 (complete trust). By executing a recommendation protocol, the network entity can determine the *Trust level* of the target, while requesting for a certain service. The accordant *Trust level* for a single target is obtained by computing the average value for multiple recommendations. Although this model does not explicitly target mobile wireless ad-hoc networks it could be used to find the selfish, malicious, or faulty entities in order to isolate them so that misbehavior will result in isolation and thus cannot continue. Unfortunately, recommendation-based *Trust-Models* are very vulnerable to *Sybil Attacks*.

3.4 Distributed Public-Key Trust Model

The core of the *Distributed Public-Key Trust Model*, examined in [18] is the use of *threshold cryptography* with the objective of avoiding the maintenance of a central Certification Authority (CA). *Threshold cryptography* implicates sharing of a key by multiple entities. The system, as a whole, has a public-/private-key pair. The private-key is distributed over *n* of nodes called *shareholders*. All nodes in the network know the system's public-key and trust any certificate signed by the corresponding private-key. Additionally, each node has a public-/private-key pair and may submit requests to get the public-key of another node or may request to change its own public-key.

The ingenious idea is that *(t+1)* out of *n shareholders* have the ability to compute the private-key by combining their partial keys but not less then *(t+1)*. In order to obtain the private-key, *(t+1)* nodes must be compromised. For the service of signing a certificate, each *shareholder* generates a partial signature for the certificate using its private-key-share and submits the partial signature to one arbitrary *shareholder*, called *combiner*. With *(t+1)* correct partial signatures the *combiner* is able to compute the signature for the certificate. Although the model offers strong security, like *authentication* of communicating nodes, it has some factors that inhibit its deployment to mobile wireless ad-hoc networks. The pre-establishment of a distributed central authority requires a huge computational complexity since asymmetric cryptographic operations are known to consume precious node battery power. Moreover, the *(t+1)* parts of the private-key may not be reachable to a node requiring authentication and subsequent asymmetric cryptographic services. Finally, the distribution of signed certificates within mobile wireless ad-hoc network settings is not sufficiently discussed and questionable. In [19] Levent Ertaul and Nitu Chavan visualize the potentialities and difficulties of *RSA*-based threshold cryptography in mobile wireless ad-hoc network settings and adapt their idea to *ECC*-based threshold cryptography in [20] for the purpose of higher efficiency. Table 1 [21] demonstrates, that key sizes can be selected to be much smaller for *ECC* than for *RSA* achieving the same level of security and protection against known attacks.

Symmetric	*ECC*	*RSA*
80	163	1024
128	283	3072
192	409	7680
256	571	15360

Table 1 *Key- size for equivalent security- levels (in bits)*

3.5 Subjective Logic Trust-Model

Josang emphasizes in [22] that public-key certificates alone do not assure *authentication* in mobile wireless ad-hoc networks, due to the missing reliable central certification. In this context, his solution introduces an algebra for the characterization of *Trust-relations* between entities. A statement such as: *"the key is authentic"* can only be either true or false but nothing in between. However, because of the *imperfect knowledge* about reality it is impossible to know with certainty whether such statements are true or false, consequently it is only feasible to have an *opinion* about it. This leads to the notions of *belief (b)*, *disbelief (d)* and *uncertainty (u)*. The relationship between these three attributes can be mathematically formulated as follows:

$$b + d+ u = 1, \{b, d, u\} \epsilon [0, 1] ^3 \qquad \textbf{(1)}$$

Triples $\omega = \{b, d, u\}$ that satisfy the above condition are called *opinions*. Figure 2 demonstrates that the condition $b + d+ u = 1$ defines a triangle. An opinion ω can be uniquely described as a point $\{b, d, u\}$ in the triangle.

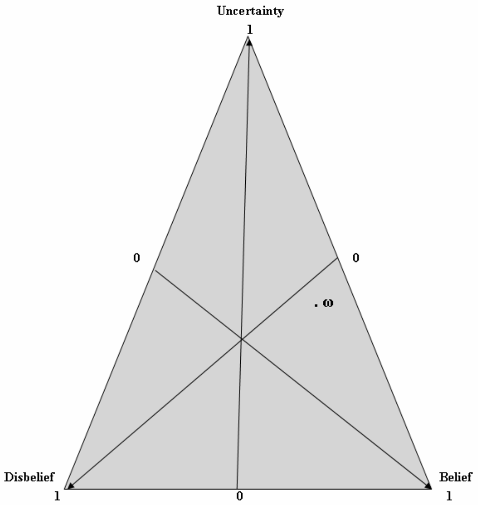

Fig.2 *Opinion Triangle*

Opinions of two different entities about the same subject may differ and are not automatically objective but subjective. The mathematical technique to characterize *subjectivity* is *Subjective Logic*. By enhancing the traditional Logic with non-traditional operators such as *recommendation* and *consensus*, the *Subjective Logic* approach is able to deal with *opinions* that are based on other entities' recommendations. Furthermore, *Subjective Logic* can produce a single *opinion* about a statement in the presence of more than one recommendation.

In the following scenario node A receives the public-key of an unknown node B and starts to examine B's public-key certificate. The certificate contains *opinions* about the key authenticity as well as *opinions* about the recommendation trustworthiness assigned by other nodes. If multiple recommended certification paths to B's key exist, A has the capability to determine the authenticity of B's key by computing the *consensus* between the authenticities obtained for each path.

By introducing *uncertainty* in *Trust* it is possible to estimate the consequences of recommendation-based decisions. However, trustworthy authentication of B's public-key requires an unbroken chain of certificates and recommendations. This is a critical condition taking the characteristics of mobile wireless ad-hoc networks into account, including the vulnerability to breakage of wireless links and the dynamically changing topology. Finally, we can conclude that the *Subjective Logic Trust* approach is not well applicable to mobile wireless ad-hoc network settings.

3.6 Ant-based Algorithm Trust-Model

The work of Tao Jiang and John S. Baras [23] presents a scheme for distributing *Trust Certificates* within dynamical mobile wireless ad-hoc networks called *ABED- Ant-Based Evidence Distribution Algorithm*. The approach is fundamentally based on the S*warm Intelligence Paradigm* used for optimization problems, like for instance the *Traveling Salesman Problem* (*TSP*) and routing [24]. The core of the paradigm is the term *stigmergy* offering a method for communication by modifying the environment. A typical example of *stigmergy* is *pheromone*. Ants, for instance, interact with each another by laying down *pheromones* along their trails. Generally, they follow those trails with the highest *pheromone* concentration aiming to find the optimal path toward their food.

The major idea of the algorithm *(ABED)* is the generation of ants everytime a certain certificate is required. The certificate serves as a *Trust* evidence of the participating entity. Each node holds its own certificate table, while each entry in this table matches with one certificate. The metric is the probability of choosing one neighbor as the next communicating entity (next hop). Two different kinds of forward ants can be mobilized to deliver the required certificate. So-called *Unicast ants* are send out to the neighbors that have the highest probability in the certificate table. *Broadcast ants* on the other hand are only sent out when there is no preference to the neighbors, if for example there is no entry in the certificate table for the required certificate. The density of *pheromone* defines the most favorable path to the required certificate. The decrease of pheromone is a function of elapsed time, which can be interpreted as a function of mobility. In this manner, a higher mobility means a faster decrease of the pheromone. A threshold value τ_0 is determined in order to assure the freshness of the *pheromone*.

Once a forward ant has found the required certificate, a backward ant is generated. This ant retraces the path of the forward ant back to the source and hands the claimed certificate. By the use of a special *Reinforcement Rule* that is comparable with a learning rule, which is the heart of the ABED, backward ants have the ability to induce certificate table modifications to perform changes.

The main weakness of the *ABED* approach is its vulnerability to Denial of Service attacks. Obviously, a compromised node has the capacity to send a huge amount certificate requests for non-existing certificates simultaneously by sending broadcast ants to all its neighbors. Each request will provoke the neighbor nodes to create broadcast ants, because they won't be able to find an entry in their *certificate table* matching the requested certificate. Consequently, the traffic load increases and may result in a network breakdown. Furthermore the attacker may launch a *Wormhole* attack considering the following scenario based on the fact that the *pheromone* deposit which is integrated in the *Reinforcement Rule* and is used to attract ants can only be modified by backward ants. In *ABED*, backward ants are only generated once a forward ant has found the requested certificate and they retrace the path of the forward ant back to the node that has requested the certificate. If the attacker's node behaves inconspicuously and generates unicast and broadcast ants in accordance with the algorithm, forward ants will find the path to the requested certificate and generate a backward ant passing the attacker's node. Right in the moment the backward ant reaches the attacker's node and wants to modify its certification table the attacker discards the backward ant and may obtain the certificate out of the backward ant's packet. As a result the requesting node won't be able to receive the certificate.

3.7 Cooperative Games and Distributed-Trust Computations

In [25] Tao Jiang and John S. Baras demonstrate that dynamic cooperative games provide a natural framework for analyzing several problems in mobile wireless networks and concentrate on the *distributed trust computation* in addition to trust distribution, explained in the paragraph above. Assuming that trust computation is distributed and restricted to only local interaction, a mobile wireless ad-hoc network is modeled as an undirected graph *(V,E)* and the edges represent connections to exchange trust information. In this context it is not necessary that two end-nodes of an edge are neighbors in geometrical distance although they have a trust relationship. The distributed trust computation model is based on elementary voting methods while only nodes in the neighborhood have the right to vote. By this technique it is possible to mark a node as trustworthy or not. A secure path in this concept is a path consisting only of trusted nodes. Unfortunately, this approach is vulnerable to attacks, where the attacker may represent multiple identities and has the capacity to generate fake recommendations about the trustworthiness of a certain node in order to attract more traffic to this node.

3.8 Trust Evaluation based on Semirings

The contribution of [26] is the introduction of a concept an indirect *Trust* relationship establishment without direct previous interactions within an ad-hoc network. By the use of the theory of semirings, the presented approach is also robust in the presence of attackers. The significant idea is to consider the *Trust inference problem* as a generalized shortest path problem on a weighted graph G(V,E), also referred to as *trust graph*. A weighted edge corresponds to one opinion. The opinion consists of two values the *trust* value and the *confidence* value that one entity has about another entity in the network. In this approach, a node relies on other nodes' past experiences and not just his own, which might be too incomplete, to ascertain if the target node is trustworthy. This solution might be very seminal in combination with an efficient *Trust Measurement* model.

4 Conclusion

Security-sensitive data and applications transmitted within mobile wireless ad-hoc networks require a high degree of security. *Trust* facilitates achieving the required protection with respect to mobility and constraints in resources of the participating devices. In this paper, we have presented *Trust* models, such as PGP as well as new approaches taking the dynamic and spontaneous nature of mobile wireless ad-hoc networks into consideration. We belief that the establishment of *Trust-Structures* turns out to be more and more important which will significantly speed-up the discovery and consequent isolation of malicious nodes in mobile wireless ad-hoc networks. Monitoring the node's past behavior in combination with recommendations of participating entities is the usual way to establish a *Trust-Metric* within a network without central and fixed stations, like a MANET. Unfortunately, most of these methods are very susceptible to *Sybil-Attacks*.

The discussed *Ant-based Adaptive Trust Evidence Distribution* Model provides the needed adaptivity to network changes and tolerance of faults in networks and offers a dynamic method to obtain *Trust* evidence in mobile wireless ad-hoc networks. We encourage and support the idea of evolutionary and ant-based *Trust* algorithms also for the collection of trust evidences in mobile ad-hoc networks. Combining both, the *Trust* evidence collection and *Trust* evidence distribution will satisfy the objective of designing an independent Trust Management system for mobile wireless ad-hoc networks.

References:

[1] P. Lamsal, Understanding Trust and Security, *Department of Computer Science, University of Helsinki, Finland* , 2001

[2] A. Josang, C. Keser, and T. Dimitrakos, Can We Manage Trust? *Proceedings of iTrust*, 2005

[3] L. Eschenauer, V. D. Gligor, and J. S. Baras, On trust establishment in mobile ad-hoc networks, *ACM Conference on Computer and Communications Security 2002: 41-47,* 2002

[4] A. A. Pirzada and C. McDonald, Establishing trust in pure ad-hoc networks, *CM International Conference Proceeding Series, Proceedings of the 27th conference on Australasian computer science*, 2004

[5] S. Buchegger and J. Le Boudec, Self-Policing Mobile Ad-Hoc Networks by Reputation, *IEEE Communication Magazine,* 2006

[6] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks*, Proceedings of the International Conference on Wireless Networks, Las Vegas*, June, 2003

[7] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Proceedings of the MobiCom '02,* September 2002

[8] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Network, *Technical Report TR01-384*, December 2001

[9] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotau, and H. Rubens, Mitigating Byzantine Attacks in Ad Hoc Wireless Networks, *Technical Report Version 1*, March 2004

[10] J. R. Douceur. The Sybil Attack. *Proceedings of the IPTP02, Cambridge, MA (USA)*, March 2002

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network, *WiSE 2003, San Diego, California, USA,* September 19, 2003

[12] G. Theodorakopoulos and J. S. Baras, Trust Evaluation in Ad-Hoc Networks, *Proceedings of the 2004 ACM WiSE`04 ,* 2004

[13] P. R. Zimmermann, The Official PGP User's Guide*, Department of Computer Science, University of Helsinki,* Finland, MIT Press, 1995

[14] J.-P. Hubaux, L. Buttyan, and S. Capkun, The Quest for Security in Mobile Ad Hoc Networks, *In Proceeding of MobiHOC,* 2001

[15] M. Blaze and J. Feigenbaum and J. Lacy, Decentralized Trust Management, *Proceedings of IEEE Conference on Security and Privacy,* Oakland, May 1996

[16] AB. Chun and A. Bavier, Decentralized Trust Management and Accountability in Federated Systems, *Proceedings of HICSS'04*, Big Island, Hawaii, 2005

[17] A. Abdul-Rahman and S. Hailes, A distributed trust model, *Proceedings of the 1997 workshop on New security paradigms*, 1997

[18] L. Zhou and Z. J. Haas, Securing Ad Hoc Networks, *IEEE Network*, 1999

[19] L. Ertaul and N. Chavan, Security of Ad Hoc Networks and Threshold Cryptography, *Wirelesscom,* 2005

[20] L. Ertaul and W. Lu, ECC Based Threshold Cryptography for Secure Data Forwarding and Security Key Exchange in MANET (I), *NETWORKING 2005,* May 2005

[21] K. Lauter, The Advantages of Elliptic Curve Cryptography for Wireless Security, *IEEE Wireless Communications* , February 2004

[22] A. Josang, An Algebra for Assessing Trust in Certification Chains, *Proceedings of the Network and Distributed Systems Security (NDSS'99) Symposium*, 1999

[23] T. Jiang and J. S. Baras, Ant-based Adaptive Trust Evidence Distribution in MANET, *Proceedings of MDC*, March 2004

[24] B. Awerbuch, D. Holmer and H. Rubens, Swarm Intelligence Routing Resilient to Byzantine Adversaries, 2004

[25] Tao Jiang and John S. Baras, Cooperative Games, Phase Transition on Graphs and Distributed Trust in MANET, *In Proceedings of 43rd IEEE Conference on Decision and Control,* Atlantis, Bahamas, 2004

[26] G. Theodorakopoulos and J. S. Baras, Trust Evaluation in Ad-Hoc Networks, *Proceedings of the 2004 ACM WiSE`04 ,* 2004