OS Issues for Coordination and Collaboration in Ad Hoc Networks

Visvasuresh Govindaswamy
University of Texas at Arlington
416 Yates Street
Box 19015
Arlington, TX
76019-0015
victor@uta.edu

Abstract

In a network all nodes need to coordinate and collaborate efficiently and securely with each other to maintain the integrity and usefulness of the network to achieve a common objective. This is especially true in Ad Hoc Networks which are actually multi-hop wireless networks. Coordination and collaboration among nodes is only possible if power consumption at these nodes are managed efficiently since significant power is consumed whenever a node or nodes either transmits or receives packets.. Reducing power consumption is clearly an important goal because battery life is not expected to increase significantly in the coming years. At the same time, this coordination and collaboration between the nodes must be achieved securely. This paper discusses two important operating system issues, power management and security, which affects the coordination and collaboration process in ad-hoc networks. It also discusses the power conserving behavior of Power Aware Multi-Access protocol for Ad Hoc Networks (PAMAS) as well as three different security approaches which deals with the coordination and collaboration of nodes within a Ad Hoc Network that is created for a meeting, a network of portable appliance and a mobile military network.

Keywords: Power Management, Security, Ad Hoc networks

1. Introduction

As Michael Schrage puts it in his book, Shared Minds [1]: "collaboration is the process of shared creation: two or more individuals with complementary skills interacting to create a shared understanding that none had previously possessed or could have come to on their own. Collaboration creates a shared meaning about a process, a product, or an event. In this sense, there is nothing routine about it. Something is there that wasn't there before". As for coordination, Leo Denise [2] writes that *"coordination* begins with an

assumption of differences. Different persons and different units create overlap, redundancy, and/or separation without coordination…Everything falls into balance, if not symmetry. Coordination is about efficiency….Coordination is a framework used to ensure that otherwise disparate forces will all pull in harness…In many cases, coordination boils down to two conditions: that people and units know what to do and when to do it; and that these people see the relationship between what they do and what the coordinated whole achieves".

In computer networks, collaboration takes place when two or more nodes creates a process of shared creation that none of the collaborating nodes had previously possessed or could have the capability of creating on their own. It is a process by which two or more nodes make a formal and sustained commitment to work together to accomplish common goals. An example of collaboration is the distribution of trust among many network nodes, rather than relying on a single node [3]. Like collaboration, coordination involves joint activity, but it allows individual node or groups of nodes to maintain their own set of goals, outcomes and responsibilities. An example of coordination occurs in [4], where a group of people that know and trust each other personally, have a meeting in a room and want to connect their laptop computers for the duration of the meeting.

An ad-hoc (or "spontaneous") network is a local area network or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network. In Latin, *ad hoc* literally means "for this," further meaning "for this purpose only," and thus usually temporary. Coordination and collaboration among nodes is difficult in this type of network. One reason for this is the rate of power consumption at these nodes. It needs to be managed efficiently since significant power is consumed whenever such coordination and collaboration takes place among the nodes. This power consumption is the result of a node or nodes either transmitting or receiving packets during the process. Reducing such power consumption is clearly an important goal because battery life is not expected to increase significantly in the coming years. At the same time, the coordination and collaboration between these nodes must be achieved securely. This paper discusses the two important operating system issues, power management and security, which affects the coordination and collaboration process in ad-hoc networks. It also discusses the power conserving behavior of PAMAS as well as three different security approaches which deals with the coordination and collaboration of nodes within a network that is created for a meeting, a network of portable appliance and a mobile military network. These two issues can easily disrupt the functionality of the entire network. The dynamic nature of the coordination and collaboration process in ad-hoc networks changes the appearances of the traditional networking. Ad-hoc networks can be described as without having an infrastructure. They do not have fixed routers or stable links. Instead, the nodes themselves route the messages. This is because the networks are created on demand, and they are often mobile. Other

network services, like name services and directory services, are absent as well. Because the networks are often wireless and mobile, they do not either have any fixed topology. Overall, ad-hoc networks are more dynamic than traditional networks. This ad hoc behavior can lead to power management and security problems whenever nodes collaborate and coordinate among each other.

The rest of the paper is as follows: section 2 presents the two issues: power management and security and section 3 conclude the paper.

2. Issues

This section is divided into two subsections. The first subsection discusses about power management and the second on security unique to ad hoc network environments.

2.1. Power Management

Whenever there is collaboration or coordination taking place between two nodes or groups of nodes in mobile ad hoc networks, significant power is consumed. Power consumption is the result of a node or nodes either transmitting or receiving packets during the collaboration or coordination process [5]. Hence, the power consumption of the Dec Roamabout radio in [6] during the transmission process is approximately 5.76 watts as compared to 15 watts of that of the radio in [7]. As for reception, the Dec Roamabout consumes 2.88 watts whereas the radio consumes 11 watts. In their idle mode, the radio consumes only 50m watts as compared to the Dec Roamabout's 0.35 watts. Moreover, in ad hoc networks, all the neighboring nodes of a transmitting node will consume power just by overhearing the transmission even though the transmission is not intended to be received by these nodes. This is illustrated as the example in Figure 1.

Here, node B is transmitting to node A which is overheard by node C and D. In doing so, nodes C and D expend their limited power by receiving a packet that was not intended for them to receive. By expending power unnecessarily in this manner affects their future coordination and collaboration with other nodes within the network. Thus, it is wise to turn off nodes C and D during the transmission from nodes B to A to conserve the power of nodes C and D. This is done in the Power Aware Multi-Access protocol with signaling for Ad Hoc Networks (PAMAS) [5].

In ad hoc networks, power consumption due to overhearing another node's transmission is very unfortunate since a packet transmission by a node might result in needless power consumption by all its neighbors resulting in poor future coordination and collaboration between these nodes.

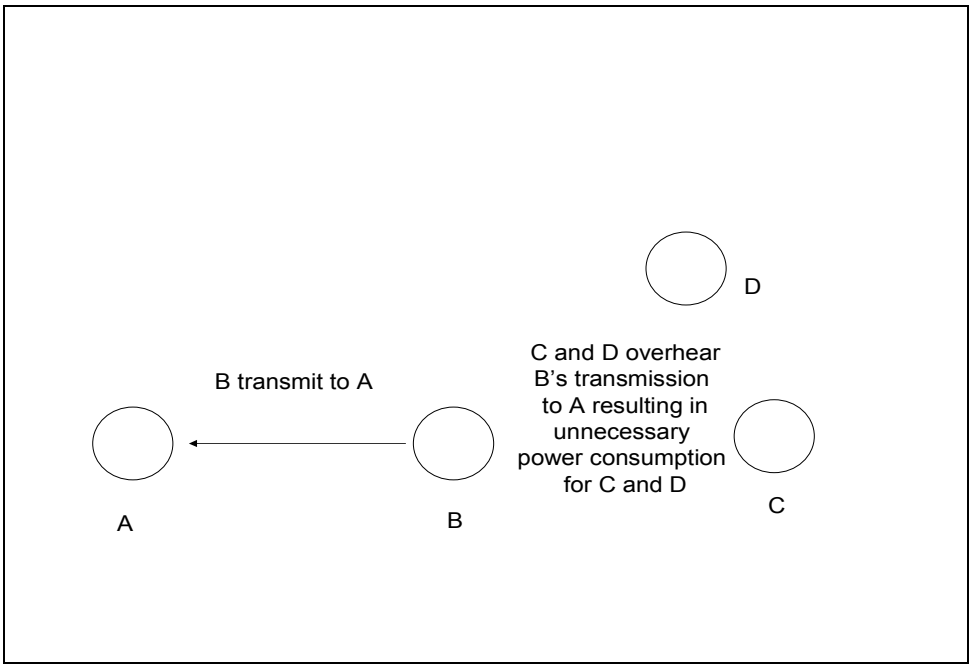

Fig. 1. Unnecessary power consumption by nodes C and D due to B's transmission to A

Consider this scenario:

1) There are n nodes in a fully connected network where a transmission by a single node will be overheard by n – 1 nodes,

2) Let T be the power consumed by a node to transmit a packet and

3) Let R be the power consumed by a node to receive a packet.

Hence, from a network point of view, the power consumed for transmitting a single packet by one of the n nodes is T + (n-1)*R. This is wastage of power within the network as the ideal power consumption, ignoring *Clear To Send* (CTS), *Request To Send* (RTS) and *Busy Tone* transmissions, should have been T + R

In the PAMAS protocol, the nodes that overhear the transmissions are required to shut down so that these nodes can conserve power and extend the lifetime of their batteries. In the above scenario, the protocol ensures that the n-1 nodes shut down for the duration of the transmission. There are two situations where there is a need for the node that is not receiving or transmitting to turn itself off. They are

1) If there is a node that has no packets to transmit, it should turn itself off if it overhears its neighbor starting to transmit.

2) If there is at least one neighbor of a node that is transmitting and another is receiving, the node should shut down. This is because it cannot transmit or receive a packet despite it's transmit queue might not be empty.

In PAMAS, the decision to power off is made by each and every node in the network independently. A node can become aware of its neighbors' transmission by listening over the data channel. In a similar manner, nodes which begins to receive a packet or in response to a RTS transmissions will emit a busy tone which will be overheard by other non-receiving and non-transmitting nodes. These non-receiving and non-transmitting nodes can then easily decide to power off.

The length of the time to remain powered off depends on how long situation 1 and/or 2 holds. However, the determination of the length of the time is complicated by the collisions within the signaling and data channel. The nodes obey the following protocol to determine the length of power-off time:

1) Let k be the duration of packet transmission that begins in the neighborhood of a node which knows the duration of the transmission. Hence, it powers itself off for k seconds.

2) Whenever one or more neighbors is in transmission when the node powers backs on, it will hear the transmissions over the data channel. In doing so, if it still has an empty queue, it will power off once more. The question now is for how long it will remain in this situation?

Figure 2 illustrates how the protocol finds a solution to this question. It shows what happens when a node powers on in the midst of transmissions by three neighboring nodes. Upon waking up, it needs to find the remaining transmission. In this case, it needs to find k_2. The node sends a *t_probe(k)* packet over the control channel where k is the maximum packet length. All nodes with transmissions completing within a time frame of [k/2, k] will respond with a *t_probe_response(t)* where t is the time to complete the transmitter's transmissions. If there is no collision, the node, on receiving the data packet, powers itself off for a time period of t seconds. If a collision does occur, it probes the time interval [3/4k, k], and so. If there is no response to the probe for [k/2.k], it probes [0, k/2]. It does this binary search until it determines the time when last transmission will end.

A simplified version of the protocol can be used. Whenever a node, on probing the time interval $[t_1, t_2]$, hears a collision, it powers itself off for the time duration of t_1. This version makes a trade-off between power and probing time since it needs to power itself back on in order to make attempts to reduce the probing time. The node could attempt to power itself off until time is t_2 instead of t_1 but this can lead to an increase in packet delays. The reason is that packet transmissions may cease soon after t_1 has elapsed and being powered off until t_2 will prevent packet delivery for this node until it is powered on once again.

Now, consider the case when nodes, having a non-empty queue, powering back on after being powered off. It transmits a RTS instead of probing since it needs to transmit a packet from its non-empty queue. If any neighboring node is transmitting, it will respond with a busy tone containing the length of the remaining transmission. If the busy tone collides with another busy tone or a CTS or some other RTS, the node attempts to probe the receivers using the same binary search algorithm but this time using *r_probe(k)*.

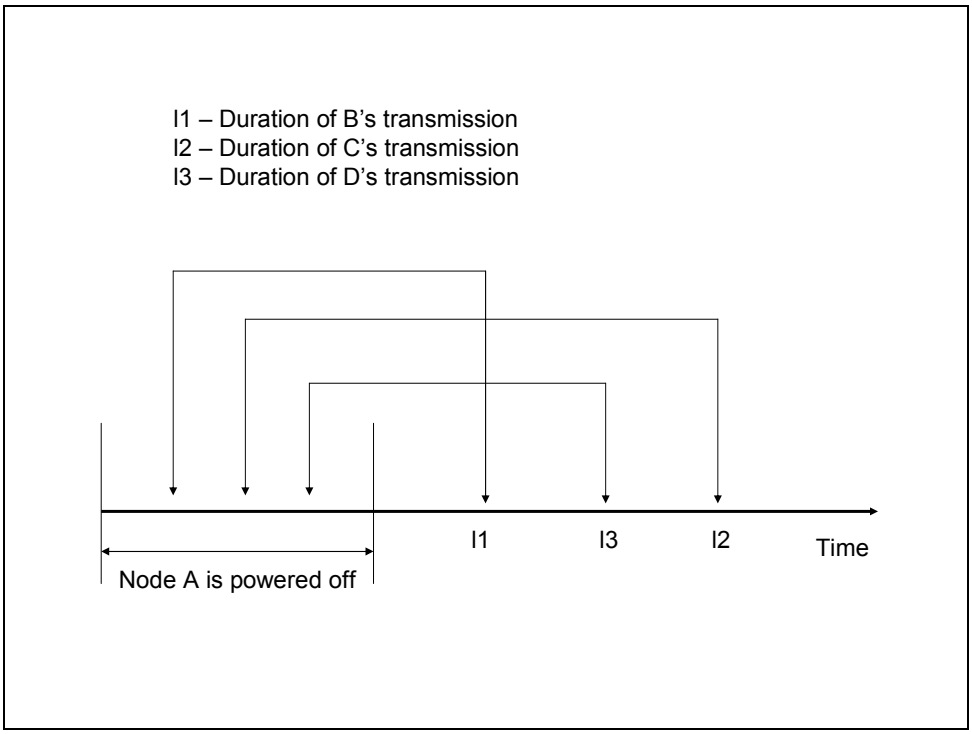

Fig. 2. Situation when a node powers back on

Then it powers itself off using

$$\text{Min } \{r, t\} \quad (2)$$

where r is the time the last receiver finishes receiving and t is the time the last transmitter finishes transmitting. The reason why the minimum is chosen in equation 2 is explained using the following two cases:

Case 1: This case deals with the situation when all the transmitters finish before the receivers finishes. This occurs when r > t. Here the node needs to power itself on so that it can receive packets from other nodes. This will reduce delays.

Case 2: This case deals with the situation when all receivers finish before the transmitters finish. This occurs when t > r. Here the node needs to power itself on so that it can transmit packets to other nodes. This again reduces delays.

There is also a chance that probe messages could get corrupted or more than one node powers on at the same time to transmit a probe message. In this situation there will be no response to the probes resulting in the nodes staying on. More research is being done in this direction.

The power conserving behavior of PAMAS were experimented upon by comparing PAMAS without power conservation and PAMAS without power conservation. The simulations were conducted in three topologies that represented most ad hoc networks. The topologies were random network, line and fully connected network topologies. The power savings were found to be more in a densely connected network than

in a sparsely connected one. In the former case, if one node transmits, more of its neighbors can power off compared to the later case. The throughput is typically lower in the former case than in latter case because fewer transmissions can go on simultaneously. Thus coordination and collaboration between nodes are more affected in densely connected ad hoc networks than those of sparsely connected.

2.2 Security

The security goals of the coordination and collaboration process in ad hoc networks are the same as that of traditional networks: confidentiality, authentication, access control, integrity and availability. However, the context is now different. In the case of security [4, 10, 11, 12], there is a lot of difficulty when dealing with this process within the ad hoc network. For example, consider the usual form of confidentiality requirement. Participant A requires the following: "only L can read the messages I send", where 'L' is a label in some name space that is meaningful to all participants. A trust a certification authority CA to correctly certify public encryption keys of entities. Participant A then achieves its confidentiality requirement by encrypting its messages using a public key for L certified by CA. This process started from a certain prior context, consisting of the well defined name space, A's confidentiality requirement, and A's trust in CA. In providing security services, one always starts from such a context. But in the ad hoc scenario, a new type of prior context is needed. The security requirement is expressed in terms of location instead of name space: "Only people present in this meeting room can read the messages I send." Thus, the usual confidentiality techniques such as the use of public keys that are certified to belong to a certain name are not relevant.

The difference is illustrated by three different scenarios and security approaches. These are a network for a meeting [4], a network of portable appliances [8], and a mobile military network [3] where nodes collaborate and coordinate to achieve a certain objective.

Securing coordination and collaboration session for a meeting

In [4], a group of people that know and trust each other personally, have a meeting in a room and want to connect their laptop computers for the duration of the meeting. There is no secure channel to connect the computers, and the participants do not have any common means to identify and authenticate each other digitally. For example, they do not share any secret keys or have any mutually verifiable public key certificate chains or have access to a trusted key distribution center. An attacker can listen to and modify all the traffic on the wireless communication channel, and may attempt to masquerade as one of the participants. One solution to the problem of the group setting up a secure session among their computers is to let the participants choose a new shared secret and use it as an encryption key to secure their communication.

The authors of [4] suggest a password-based authentication protocol that is derived from the so called *encrypted key exchange* (EKE) protocol [9]. In EKE, two participants, who share a secret, create together a

session key. The secret, or password, can in fact be weak. Nevertheless, anyone who does not know the password cannot successfully participate in the protocol. Finally, EKE provides perfect forward secrecy: even if an attacker later finds out the password, he or she cannot find out the previous session keys. Hence the messages of the past sessions remain secret.

In the group version of EKE all the participants contribute to the session key. This ensures that the resulting key is not selected from too small a key space even if some participants would try to do that. An attacker, who tries to participate in the protocol and sends some random messages, cannot prevent the construction of the key. As in the original EKE, only the participants who know the original password learn the resulting session key. The secure connections between the participants are created from a manually exchanged password. Hence, no support infrastructure is needed. This will enable the nodes within this network to coordinate and collaborate securely.

Securing coordination and collaboration in networks of portable appliances

In [8], Stajano and Anderson study ad-hoc networks where the nodes are (personal) devices that can communicate with each other over a wireless channel. A special example is a thermometer that broadcasts the temperature to authorized recipients. The device can have multiple serialized owners, and the association between the device and the present owners should be secure and transient.

System constraints and low physical security are characteristic of ad-hoc networks of portable appliances. The devices on the network probably operate with batteries and have a small CPU. Hence, the computing power of a node is small and computations are slow. To save the batteries, the nodes go to sleep whenever possible and turn on their receivers only periodically. This brings high latency to the network. Low physical security is due to the fact that the devices could be physically located far from the parties they serve and be left to their own fate. An attacker could possibly modify or forge a node physically. In the case of the thermometer, the attacker may just change the sensor to an invalid one. All this makes secure coordination and collaboration very difficult.

The system constraints have impact on the methods for authentication, integrity and confidentiality. Because of the low computational power of the nodes, it may not be feasible to implement public key cryptography. Besides, no secure protocol is of any help if the secret information can physically be recovered from the unprotected nodes. Networks are also vulnerable to denial-of-service attacks. Malicious battery exhaustion could be enough to achieve denial of service.

The authors present the *resurrecting duckling* security model to solve the secure transient association problem. Like a duckling considers the first moving object it sees as its mother, in the same way a device would recognize the first entity that sends it a secret key as its owner. The duckling will only die when so instructed by its mother: thus only the current authorized user may transfer control of the device. When necessary, the owner could later clear the imprinting and let the device change its owner. The imprinting -

sharing the key - would be done in a physical contact. In the case of several owners, the secret key is transmitted in plaintext when the device is in pre-birth state. It can be transmitted with different access rights, the imprinting could be done several times with different keys. In this manner, it could be possible to create a hierarchy between the owners, or prioritize the service requests. Tamper resistance, or tamper evidence, may protect against physical threats of the nodes. This technique will enable the nodes within a network that requires high performance, low power consumption and with minimum security to coordinate and collaborate.

Securing mobile military networks

A mobile military ad-hoc network is both securities sensitive and easily exposed to security attacks [3]. Not only the information passing from a node to node is confidential, but the wireless traffic itself can reveal the location of a target to the enemy. The nodes, roaming in a hostile environment with little physical protection, might be compromised, which increases the possibility of attacks inside the network. Finally, the network is highly dynamic both in its topology and membership. Nodes frequently join and leave the network, and detecting compromised nodes also changes the trust relations. In [3], the authors concentrate on the goals of secure coordination and collaboration to achieve security, and creating a distributed, asynchronous key-management service.

Because of the possibility of the nodes be compromised, the network should not have any central entities but a distributed architecture. This protects against denial-of-service attacks and major information disclosure. If public key cryptography is involved, a central Certification Authority is problematic.

The authors present a distributed key management where the private key of a trusted service is divided to *n* servers. To create a signature with the private key, at least *k* out of the *n* servers need to combine their knowledge. Combining the shares would not reveal the actual private key. The correctness of the signature would, as usual, be verifiable with the public key of the service.

The method is called threshold cryptography: an *(n, k)* threshold cryptography scheme allows *n* parties to share the ability to perform a cryptographic operation (e.g., creating a digital signature). Any *k* parties can perform the operation jointly, whereas it is infeasible for at most *k-1* parties to do so. If we suppose that at most *k-1* servers can be compromised at time, a false signature cannot be created.

The key management service also employs share refreshing and is scalable to changes in the number of servers. Periodical share refreshing creates new shares of the private key, so that an adversary cannot collect information about *k* shares over time. The system is also scalable and adapts itself to the changes in the number of participating servers. This technique will enable the nodes within a network that requires high levels of security to coordinate and collaborate.

3. Conclusion and Discussions

In the previous section, this paper discusses how important the two issues are for the collaboration and coordination process in ad hoc network. Failure to address these issues might result in the collapse of the network. Excessive and unnecessary power consumption will lead to deterioration in battery life of the nodes. This will result in poor coordination and collaboration among the nodes. Nodes will not have sufficient power to route, receive and/or transmit messages unless their batteries are replaced regularly.

As for secure coordination and collaboration between nodes, authentication that relies on public key cryptography and Certification Authorities may not be accomplished in ad-hoc networks. Either the nodes do not have a common history and supporting infrastructure, or the lack of physical security and the threat of denial of service do not allow the network to have any central entities. It may also happen that the computational power of the nodes is too weak to support such measures that demand excessive power consumption.

The dynamic topology prevents creation of firewalls [13, 14, 15]. Inside and outside loose their meaning in ad-hoc networks, while firewall assumes that the inside network is physically safe. Access control to the network and to the resources that may be used in the coordination and collaboration process may need different methods.

Weak physical security and the vanishing distinction between ‘inside’ and ‘outside’ also affects on how and where the adversary node might be. There should be safeguard against coordination and collaboration with a hostile node. There will be attacks initiated from inside the network by trusted nodes - or at least the users cannot trust this would not happen. This makes the distinction between authentic and forged information more difficult, and the risk that apparently authentic information is in fact not authentic at all, is increased. How can the nodes be sure about the authenticity, or do the nodes have to deal with variable degrees of assurance in order to coordinate and collaborate?

Not only the ad-hoc network topology, membership and trust relations are dynamic, but it seems that also the information ad-hoc networks produce and transmit has a dynamic nature. It contains news about the environment of the nodes, information about the changes in the network, and messages exchanged in the sessions of the parties - information that is valuable only at the moment. Traditional network services like databases, file systems and document servers, static information in other words, seem less characteristic to ad-hoc networks.

Fortunately, it is not always the case that all the traditional security assumptions fail. In the examples of a meeting, network of portable appliances, and military network, the lack of infrastructure was worst in the meeting scenario but physical security was not a problem. On the other hand, mobile military networks have at background an organization with a long history, trust, and hierarchy.

Since the functionality, capabilities and purposes may vary between coordination and collaboration in different ad-hoc networks as well as between the nodes in an ad-hoc network, it is questionable, how general solutions for power management and security are possible to create in the first place. More work should be done to identify the most probable types of coordination and collaboration within ad-hoc networks in the future, and what kind of network infrastructure, power management and physical security are necessary for efficient coordination and collaboration to be available in these networks.

4. References

[1] M. Schrage, "Shared Minds", New York: Random House, 1990.

[2] L. Denise, ''The Power of Collaboration'', Perdido Magazine, Volume 6, Number 1, Winter 1999.

[3] L. Zhou, Z. Haas, Zygmunt J., "Securing Ad Hoc Networks", IEEE Network, vol. 13, no. 6, November/December 1999.

[4] N. Asokan, & P. Ginzboorg, "Key Agreement in Ad-hoc Networks", Elsevier Preprint, 2000.

[5] S. Zdonik, M. Franklin, R. Alonso, S. Acharya, "Are "disks in the air" just pie in the sky?", *IEEE Workshop on Mobile Computing Systems and Applications,* Santa Cruz, CA, pp. 12-19, December 1994.

[6] H.S. Wilf, Algorithms and Complexity, Prentice Hall, 1986.

[7] M. Stemm, P. Gauthier, D. Harada, "Reducing power consumption of network interfaces in hand-held devices", *3rd International Workshop on Mobile Multimedia Communications,* September 25-27, 1996.

[8] F. Stajano, R. Anderson, "The Resurrecting Duckling: Security issues for Ad-hoc Wireless Networks", *Proceedings of the 7th International Workshop on Security Protocols*, Lecture Notes in Computer Science, Springer-verlag, Berlin Germany, April 1999.

[9] M. B. Steven and M. Michael, "Encrypted key exchange: Password-based protocols secure against dictionary attacks". *Proceedings of the IEEE Symposium on Research in Security and Privacy*, May 1992.

[10] You W., "Authentication and Other Security Issues", Virginia Polytechnic Institute and State University, 2001.

[11] Ateniese, Giuseppe & Steiner, Michael & Tsudik, Gene, "New Multiparty Authentication Services and Key Agreement Protocols", *IEEE Journal on Selected Areas in Communication*, vol. 18, no. 4, 2000.

[12] Becker, K. & Wille, U., "Communication Complexity of Group Key Distribution, *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pp. 1-6, San Francisco, CA USA, 1998, ACM Press.

[13] Amoroso, E., "Fundamentals of Computer Security Technology", Prentice-Hall International, Englewood Cliffs, NJ, 1994, 404p.

[14] Steiner, Michael & Tsudik, Gene & Waidner, Michael, Diffie-Hellman "Key Distribution Extended to Group Communication", *In 3rd ACM Conference on Computer and Communications Security*, pp. 31-37, New Delhi, India, 1996, ACM Press.

[15] Gollmann, D., "Computer Security", John Wiley & Sons, 1999, 320p.