ROCHESTER INSTITUTE OF TECHNOLOGY

A PROJECT PROPOSAL SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE

Security in Ad hoc Networks

Author:
Ankit JOSHI

Supervisor:
Dr. Hans-Peter BISCHOF

Reader:
Dr. Stanislaw RADZISZOWSKI

Department of Computer Science

B. Thomas College of Computing and Information Sciences Rochester Institute of Technlology

Rochester, New York
February 27, 2013

MS Project Proposal

Abstract

Wireless ad hoc networks are decentralized types of networks. These networks are called as ad hoc networks because they do not depend on any predefined infrastructure for communication purpose. The nodes in the network themselves help in routing the packets and providing the security for communication. Due to the absence of any wired connection or any third-party authentication method, these types of networks are more vulnerable to the attacks.

This project will be helpful to create a secure routing protocol with the help of the security key management system for the group communication of the ad hoc networks. For the testing purpose, the Network Simulator (NS-2) would be used which will help in studying the performance of the applied method and test it against other similar security mechanisms. The comparison between the proposed method and the existing methods would be done against the communication overhead and the time required to generate and regenerate the key

Contents

List of Figures

1 Project Introduction

1.1 Introduction

The nature of the wireless ad hoc networks make them more prone to the security attacks then the traditional wired-networks. The ad hoc networks do not have any pre-existing infrastructure, nor do they have any centralized authorization system which would help in securing the network. The members or nodes of the network themselves are responsible in securing the communication and also in routing the package from source node to the destination node. The nodes are responsible to generate the security keys, encrypt and decrypt the packets, and make sure that the key is not available to any other node outside the network. A simple structure of a wireless ad hoc network is displayed in the figure below: The wireless ad hoc

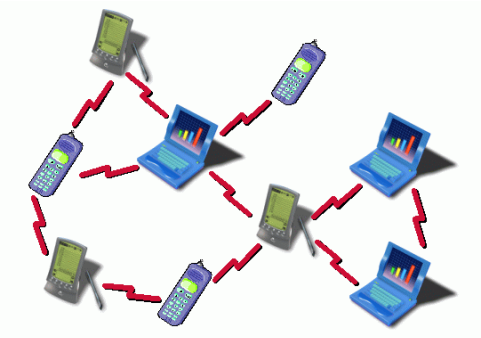

Figure 1: Structure of Wireless-Ad hoc Network

network can be categorized into: (1) *Mobile Ad hoc Network (MANET)*, (2) *Wireless Mesh Network (WMN)*, and (3) *Wireless Sensor Network (WSN)*. The mobile ad hoc networks are more difficult to handle due to the mobile nature of the nodes. The nodes in the network are not fixed at any given time, they may be moving from one place to another and at any speed. This makes the network more vulnerable and difficult to be secured more due to the mobile nature and also due to the less physical security of the nodes.

1.2 Background

Mobile ad hoc networks is called as the next generation of the original wireless ad hoc network. Wikipedia defines such networks as “Mobile Ad hoc Network (MANET) is a self-organizing infrastructure less network of mobile devices con-

nected by wireless" [22]. The nodes in the network are free to move from one location to another and also this movement is in an unpredictable fashion. This requires reconfiguring the network on the fly in order to handle the dynamic topology. The lack of centralized authority makes the network vulnerable to attacks like: interception, interference, and passive eavesdropping. The nodes may also become selfish and not forward any packets to another node. Routing becomes one of the most important aspect for mobile ad hoc networks which would help in finding the proper route from the source to destination. Securing the route becomes another important aspect, which would help in avoiding the attacks on the nodes. Several routing algorithms have been proposed in the literature, such as Ad hoc On-demand Distance Vector (AODV) Routing Protocol, and its variations like Mobility-Aware AODV Routing Protocols (MA-AODV) [8], Multicast Routing Protocol [21], Hyper cube Based Team Multicasting Routing Protocol [12], Cluster-based Routing Protcol [2], etc... Also few security methods have been proposed like Symmetric Key management, Tree-based group key management [16], K-Dimensional Tree based key management [17], Group Key management system [4], etc... The main challenges these algorithms have to suffer are:

- *Wireless Links:* The Mobile Ad hoc Networks (MANETs) do not have wired connection unlike the traditional wired networks. Thus, centralized authentication mechanism is not possible for MANETs. This makes them vulnerable to passive attacks like sniffing, or active attacks like injecting malicious code in the message, selfishness, etc...

- *No Infrastructure:* There is no external infrastructure for the routing or security purpose. The nodes are themselves responsible sending the packets from source to destination.

- *Scalability:* Group key management becomes a necessity since, the number of nodes joining or leaving the network is not restricted or fixed.

- *Mobility:* The nodes in MANETs are mobile in nature, thus, they are not at any fixed position at any given time. Also, these nodes can move from one place to another at varying speed. This makes the key generation and regeneration more difficult and thus, a mechanism which can handle such mobility is required which can provide a better key generation and regeneration model.

- *Limited Power:* The mobile devices do not have high power. the energy, bandwidth and CPU of these devices may be limited. Also, such devices may have

limited memory.

1.3 Related Work

The literature specifies many cryptographic algorithms used for security mechanisms for the mobile nodes in the mobile ad hoc networks. Most of the methods used depends on the key management mechanism. These key management models use public key infrastructure and private key infrastructure. Public key models use asymmetric key algorithms, whereas, private key models use symmetric key algorithms. Also, many of the asymmetric key algorithms use the public/private key pairs for the security mechanism, where, public key is visible to all the nodes in the networks, whereas, private key is shared only between the source and the destination. Multicast key distribution methods have been proposed in many papers. The advantage of multicast communication over regular unicast communication is that it helps to communicate between more than one node at a time. This helps in reducing the communication overhead. Few of the papers like [21], [12], [19], [8] have proposed routings protocols. The most common routing protocol used is the AODV routing protocol. Paper [12] proposes a Hypercube Based Team Multicasting Routing Protocol (HTMRP) which provides scalability, robustness, high availability, and good load-balancing with the help of the team multicast and hypercube mechanism. In this model, the nodes are organized in the teams depending on the common interests of the nodes. The hierarchical multicasting protocol is used to organize the nodes with the help of the three-tier multicast routing paradigm. The bottom-most tier is the Landmark Tier, where the teams are formed, the middle tier is the Hypercube Tier, which comprises of the three-dimensional hypercube. This tier consists of the team leaders of the groups formed in the landmark tier. The top-most tier is the Mesh tier, which consists of hypercube as one mesh node. This helps in intergroup communication and provides logical connections between different hypercube. this helps in better connection between the nodes and thus, helps to improve the delivery ratio. Another paper [2] proposes the fully distributed mechanism. This model divides the network into number of groups, which are lead by their respective group leaders and these groups are further divided into subgroups called as clusters, which are led by their cluster heads. Dividing the network into smaller groups and clusters, makes it easier to generate and regenerate the keys. This method is efficient, as key regeneration will be required only for the cluster or group from which the nodes leave or join, and the other nodes in the network are

not required to regenerate the key. The only minus point in this method proposed in [2], is that, the number of nodes per group should be smaller to get the best communication time. With more nodes per groups, the key generation time would be more. A similar method is proposed in [19]. The difference between this method and the above method is that, in this method, the clusters are formed in parallel. In this proposed model, every cluster has more than one cluster head called as Council. The council members are the ones which have direct connection with each other. So, it becomes necessary to have a particular number of cluster heads to generate the security key. According to the authors of paper [19], using this model, it becomes difficult for the attacker to compromise the cluster even if one or more clusters are compromised but less than (k,n-k+1), where, k is the number of clusters required to generate the key and n is the number of clusters in the Council. The number of clusters required i.e. k should be defined in such a way that it is greater than 1 and less than n. The reason behind this is that:

- If k is selected to be 1, then it becomes easy to compromise the network by just compromising one single cluster head. This is opposite to the hypothesis set by the authors in the paper.
- If k is same as n, then all the cluster heads are required to generate the key. This makes the network most secured and is useful for military purposes where secured communication is the necessity. But for regular use, this becomes difficult and requires more communication overhead and more key generation and regeneration time.

Thus, k should be such that $1 \leq \mathrm{k} \leq \mathrm{n}$ so that it provides the balance between security and availability [19] A Mobility-Aware AODV (MA-AODV) routing protocol has been defined in [8]. This method helps the traditional AODV protocol to be mobility aware, thus, helping to provide better routes. This model makes use of the traditional AODV routing protocol i.e. sending the Route Request (RREQ) packets and the Route Reply (RREP) packets to find the route. Two separate methods i.e. Per-Hop Mobility-Aware AODV (PH MA AODV) routing protocol and the Aggregate Mobility Aware AODV (Agg-AODV) routing protocol have been described. The difference between the two mechanisms is that, in PH-MA-AODV, the nodes themselves decide if they want to be included in the route and in Agg-AODV, the destination node decides if the nodes are required in the route depending on the mobility level of the nodes i.e. high or low. Such methods help the routing procedure to be more reliable and stable. A location based routing protocol is described in [13].

This method uses the Global Positioning System (GPS) to locate the nodes and keep track of their location. This method is useful for getting the accurate location of the nodes in the network but consumes more power. Also, the memory requirement of this method is more since there is lot of redundancy and also the communication overhead is at a higher side. This method is not possible to be used for mobile nodes due to the less power and memory of these nodes. The above papers have all proposed different routing protocols. Let's look at few paper which have proposed the key management systems. According to [16], the key management systems can be categorized into: (1) *Centralized group key management protocols*, (2) *Decentralized architecture*, and (3) *Distributed key management protocols*. It also describes few rules of these security mechanisms such as: (1) *Forward Secrecy*, (2) *Backward Secrecy*, (3) *Key Independence*, and (4) *Group key secrecy*. Various security mechanisms have been proposed in the literature in order to prevent the attacks and take care of the above mentioned points. Paper *survive* provides a mechanism where, the author says, in order to make the network secure and avoid the delays caused by the malicious nodes, it is necessary to provide the keys to the destined nodes even when few of the network members are compromised. This method used the Certificate Revocation List (CRL) which updates the identities of the nodes that are compromised. In this way, the non-compromised nodes are made aware of the compromised nodes and thus, helps in preventing these nodes to receive the network key.

Another simple method known as *Polynomial-based conference key* has been proposed in [7]. This method does not have complicated calculations, also, neither the source, nor the destination needs to communicate to each other before exchanging the packets. Both, the source and destination can generate the required keys for encryption and decryption without communicating with each other with the help of the following formula:

$$f(x,y) = 1+2(x+y)+3xy \text{ [7]}$$

where "x" is the source node and "y" is the destination node [7]. With the help of this formula, x and y can calculate the unique keys to communicate with each other without the need to communicate prior. This helps in keeping the key secret and private and thus, less chances of compromising the node. Also, communication overhead is reduced and key regeneration is not required. Many other papers have proposed tree-based key distribution system such as *Hierarchical Approach* in [2], *Multicast Tree* in [21], *Key Management using K-Dimensional Tree* in [17], etc...

All these methods are very useful but most of them suffer from communication overhead and also the key generation and regeneration process for them is required regularly at many levels. The best of the tree-based key management model is the one proposed in [17]. It helps to organize the keys in form of a binary tree. The key generation does not require much time and also the key regeneration (when any nodes join or leave the network) is required only for the child nodes and the parent nodes of the tree. No other nodes are required to regenerate the keys. Also, this is the only tree-based method, which divides the network into groups. Thus, helping to reduce the communication overhead and the key generation and regeneration time. Other papers like [4] describe cluster based group key management protocols, where the network is divided into clusters and keys are generated for every cluster. A method described in [3] is suitable for smaller networks but has more security. For a node to communicate with another node in different cluster, it has to send the packets through its neighboring nodes, which require to send the packets to another cluster only through the gateway nodes which contains the keys for both the clusters it is between. This gateway node then decrypts the packets using the key of the first cluster and then again encrypts the packet using the key of the second cluster. This process continues till the packet reaches its destination. There is more communication overhead, but the key generation and regeneration process takes very less time.

2 Project Objectives

2.1 Hypothesis

Most of the existing methods use either AODV routing protocol or an n-party Diffie-Hellman security algorithm. Most of the existing models have either large communication overhead or the key generation time and regeneration time required is high. This results in delayed communication over the network. I propose to find a solution and create a secure routing protocol with the help of the multicast AODV routing protocol and n-party Diffie-Hellman algorithm which would have the least possible communication overhead and also the key generation and regeneration time would be minimum thus, requiring less memory, and also the communication delay won't be much. Only providing a better routing protocol or by securing the communication between the nodes of a network is not enough. It become necessary to provide both, a better routing protocol which can result in good and better delivery ratio and

also a secure communication which can help to avoid the attacks.

2.2 Approach

As mentioned in the above sections, many routing algorithms and security models have been proposed in the literature. Most of the papers use either a routing protocol or a security mechanism to improve the results. I would like to use a Multicast Routing Protocol as shown in figure 2, which would provide a better routing mechanism and for securing the packets and communication, I would like to use the *n*-party-Diffie Hellman algorithm which supports generating keys simultaneously for different nodes. For the multicast routing protocol, factors such as delivery ratio,

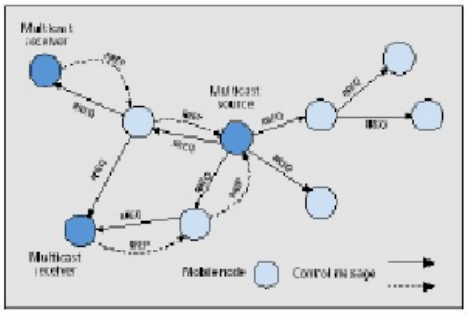

Figure 2: Multicast routing

mobility of the nodes in the network, delivery time, will be considered and analyzed. And for the security reasons, the communication overhead, key generation and regeneration time would be considered and analyzed. Once, all the parameters are defined and the results are calculated, the proposed model will be tested using a network simulator with all the possible parameters. Also, it will be tested with altered parameters. The testing of the model on the network simulator will be the major part in the project. It will be able to test the mobility of the nodes, how the routes are affected when the mobility is high or low, how the keys are generated or regenerated and how much time is required when nodes frequently join or leave the network, also it will be able to calculate the communication overhead for less as well as high number of nodes in the network.

2.3 Evaluation

The evaluation for this study will be done by performing the tests using a network simulator. The parameters used in the simulation process would be varied for testing the proposed model in different environments and with varying inputs. The main factors that will be considered for the testing and evaluating purpose are:

- **Delivery Ratio:** Packet delivery ratios of 100% in Mobile Ad hoc Networks cannot be achieved but packet delivery ratios in access of 99% are possible in most cases. Delivery of all packets is a minimum requirement for any reliable multicast mechanism, but it is possible that not all the packets are delivered as per the requirements. Achieving higher packet delivery ratios in a MANET is not trivial. In literature, many methods have been proposed which have higher packet delivery ratios like extensions for AODV. *Packet Delivery Ratio* can be defined as the percentage of received packets, relative to the total number of packets ideally received. To improve the packet delivery ratio, two distinct approaches are possible:
  - *Reduce the number of target nodes:* Rather than broadcasting the data to every node, send the data only to the intended nodes.
  - *Reduce the number of re-broadcasts:* Fewer broadcasts will result in the wireless media being less busy, increasing the chance that the packet is successfully transfered, rather than being dropped.

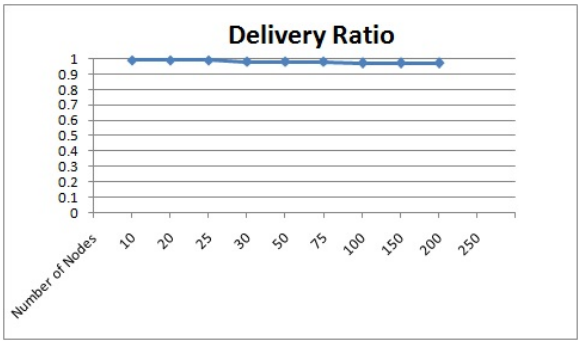

Figure 3: Delivery Ratio

Figure 3 shows an assumption of how the proposed model would give the delivery ratio. The x-axis consists of the number of nodes and the y-axis shows the ratio depending on the number of nodes. The proposed model would pro-

vide a delivery ratio even for the larger network but it may have better ratio for smaller networks.

- **Mobility of nodes in the network:** The mobility of nodes in the simulation can be assumed to be for the mobile nodes with the people walking on the street. This means the speed of the mobile nodes will not be very high. Here, the packet delivery ratio can be higher as compared to the ratio when the mobility of the nodes is higher for example when the nodes are moving in car with higher speed. For our purpose, we can test the delivery ratio for both, slow speed and high speed. The NS-2 simulator, has the built-in *Random Waypoint* mechanism which helps in changing the speed of the nodes and the time interval in which the nodes moves or remains constant at one location. The nodes can move or remain constant. The time for the node to remain constant can also be changed as per the requirements. All these changes can be done with the help of the *random waypoint* method provided by the ns-2 simulator. Figure 4 illustrates the assumption for the proposed model about how the

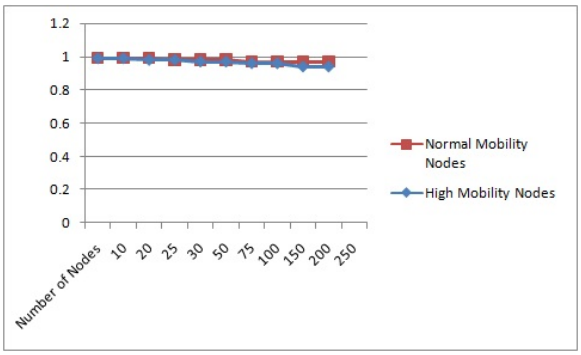

Figure 4: Delivery Ratio depending on the Mobility of nodes

delivery ratio may differ for nodes with higher mobility with the nodes with normal mobility. As the figure shows, there would not be much difference in the delivery ratio even for the nodes with high mobility. This can be done with the help of the routing mechanism which would provide proper position of the nodes in the network.

- **Size of network:** The size of the network also plays an important role to measure the packet deliver ratio. Bigger the network, more the number of nodes and more the communication overhead. The packets may or may not get dropped depending on the strength of the nodes and the network. But the model must be able to handle larger number of nodes in order to provide better

efficiency and better delivery ratio.

- **Communication Overhead:** Communication overhead is measured in the form of the number of packets transferred between each node over a period of time. In larger networks, if every node communicates with each other for forming the key, the communication overhead would be more. But if the network is divided into groups, the communication overhead will reduce significantly. Also if the number of nodes per group is not more, the overhead will be less. With larger network, the overhead may increase to a certain extent but that would not create any problems if the network is efficient and divided into groups or clusters. The communication overhead for the proposed model

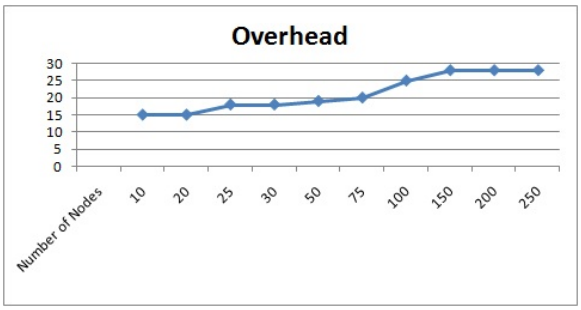

Figure 5: Communication Overhead

would be as minimum as possible. It may have higher communication overhead for larger networks but even that would not create any delays in the delivery of any packets. The communication overhead can be reduced by having more number of groups and by limiting the number of nodes per group. This will help the communication overhead to be constant.

- **Key generation and regeneration time:** The key generation time depends on the number of nodes in the network. Higher the number of nodes, the time required to generate the key would be more. But again, if the network is divided into clusters or groups, the time required to generate key would be less since all the clusters or groups would be simultaneously generating keys and a cluster head or group leader would be responsible to maintain the keys. This also helps in reducing the time required to regenerate the key when a node joins or leaves the network as only the cluster in which the node joins or leaves has to recalculate the key. Other nodes in the network need not recalculate the key.

Some additional influential parameters may also be considered, which may be identified during the study and while the implementation is in process. Many models have been proposed earlier to make the mobile ad hoc networks secure and efficient to communicate. The aim of this project is not to just secure the network, but also to make sure the packets are delivered to the destination node correctly with higher delivery ratio. The accuracy of the delivery ratio would depend directly on the mobility of the nodes. So, the proposed scheme has to consider the mobility of the nodes and provide a better delivery ratio. Also, with high mobility, the network may be more vulnerable. So the security method proposed must take in consideration of the mobility and will provide a better and efficient key generation method. After the completion of the study, we will have a complete analysis for different factors and parameters.

3 AODV

The Ad-hoc On-demand Distance Vector Routing (AODV) protocol is a widely used protocol for mobile ad hoc networks. AODV uses a broadcast route discovery mechanism. The main method used by AODV for path discovery is the use of the RREQ (Route Request) and RREP (Rout Response) messages. Also, it helps in minimizing the number of broadcasting message. AODV prepares loop free routes. The multicast AODV is nothing but an extension to the traditional AODV. Multicast AODV also utilizes the same method to communicate and find routes i.e. by using the RREQ and the RREP messages. The paper [18] proposes an improved MAODV protocol which does not only have the functionality of multicasting but also reliability capability in high mobility rate and large network area [18]. IMAODV creates bi-directional shared multicast trees and these groups are maintained until the nodes exist in the network. The multicast trees are formed as the groups are formed and nodes start joining the network. These trees are established independently in each partition, and trees for the same multicast group are quickly connected if required. But the only drawback of IMAODV is that it has more end-to-end delay for communication between nodes. A simple algorithm for validating the Source node is as follows:

Algorithm 1 Validation of the Source Node

// t_r denotes the time when the RREQ is received
// ts denotes the issue time of the RREQ
//D- propagation delay 1. Assume node 'k' receives a RREQ at t_r
2. **if** ts + d $<$ t_r **then**
3. Discard the RREQ
4. **else**
5. **if** (forwarding node is a trusted node) **then**
6. Buffer the RREQ packet and store forward node ID in request table.
7. Wait (for group authenticating key to be disclosed).
8. **if** (source node 'i' has a valid group member certificate) **then**
9. Send the RREP packet with the following details;
10. Append the tree key and reply node ID
11. Encrypt with the source node public key.
12. **else**
13. Discard RREQ
14. **end if**
15. **else**
16. Report the unauthorized node to CA.
17. **end if**
18. **end if**

4 Project Deliverables

The project deliverables will comprise of the following:

- A simulation of the model for both routing and security algorithms.
- A Final Masters' Capstone Report including the entire idea, implementation, test cases, final results and the conclusion of the project.
- Final report Powerpoint Presentation.

5 Current Status

- Initial and Revised Proposal
- Parameters defined.
- Researched on the required algorithms.

6 Proposed Roadmap

March 2012	Background Research
April 2012	Collecting information regrading the network simulators
May 2012	Finalizing the parameters and factors necessary
June 2012	Implementing an algorithm for routing and security purpose
July 2012	Testing the algorithms on the network simulator
August 2012	continue the testing and analyze the results, Report documentation
September 2012	Tentative Defense Date

References

[1] Cryptool portal - free download for cryptool simulator. [Online]. Available: http://www.cryptool.org/en/

[2] R. A. and K. C. Shet, "Hierarchical approach for key management in mobile ad hoc networks," *CoRR*, vol. abs/0910.0227, 2009.

[3] M. AMAD, D. AISSANI, and A. MEDDAHI, "Multi group key agreement mechanism for mobile p2p wireless networks," 2011.

[4] Q. Chen, X. Lin, S. Shen, K. Hashimoto, and N. Kato, "A group-based key management protocol for mobile ad hoc networks," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 30 2009-dec. 4 2009, pp. 1 –5.

[5] M. Dasgupta, S. Choudhury, and N. Chaki, "A secure hypercube based team multicast routing protocois (s-htmrp)," in *Advance Computing Conference, 2009. IACC 2009. IEEE International*, march 2009, pp. 1265 –1269.

[6] R. Gordon and D. Dawoud, "Trust establisment in ad hoc networks by certificate distribution and postponed vertification," 2011.

[7] A. Gupta, A. Mukherjee, B. Xie, and D. P. Agrawal, "Decentralized key generation scheme for cellular-based heterogeneous wireless ad hoc

networks," *J. Parallel Distrib. Comput.*, vol. 67, no. 9, pp. 981–991, Sept. 2007. [Online]. Available: http://dx.doi.org/10.1016/j.jpdc.2007.05.009

[8] Y. Khamayseh, O. Darwish, and S. Wedian, "Ma-aodv: Mobility aware routing protocols for mobile ad hoc networks," in *Systems and Networks Communications, 2009. ICSNC '09. Fourth International Conference on*, sept. 2009, pp. 25 –29.

[9] B. Lehane, L.Doyle, and D. O'Mahony, "Share rsa key generation in a mobile ad hoc networks," 2011.

[10] P. M. M. B. Mutanga* and M. O. Adigun, "Towards auto-configuring routing protocols for wireless ad-hoc networks," 2011.

[11] I. C. M. S. Bouassida and O. Festor., *Internation Journal of Network Security IJNS.*, vol. 6, no. 1, pp. 67 – 79, Jan. 2008.

[12] R. Manoharan and P. Thambidurai, "Hypercube based team multicast routing protocol for mobile ad hoc networks," in *Information Technology, 2006. ICIT '06. 9th International Conference on*, dec. 2006, pp. 60 –63.

[13] R. Melamed, I. Keidar, and Y. Barel, "Octopus: a fault-tolerant and efficient ad-hoc routing protocol," *Wirel. Netw.*, vol. 14, no. 6, pp. 777–793, Dec. 2008. [Online]. Available: http://dx.doi.org/10.1007/s11276-006-0013-6

[14] K. Needels and M. Kwon, "Secure routing in peer-to-peer distributed hash tables," in *Proceedings of the 2009 ACM symposium on Applied Computing*, ser. SAC '09. New York, NY, USA: ACM, 2009, pp. 54–58. [Online]. Available: http://doi.acm.org/10.1145/1529282.1529292

[15] E. S. A. A. L. Nogueira, M. Silva, "Survivable key management on wanets," *IEEE Wireless Communications*, pp. 82 – 88, dec 2011.

[16] G. Patnaik and M. Gore, "Tree-like peer-to-peer symmetric key management in mobile ad hoc network," in *Networks and Communications, 2009. NETCOM '09. First International Conference on*, dec. 2009, pp. 196 –201.

[17] A. Renuka and K. Shet, "Key management using k-dimensional trees," in *Advanced Computing and Communications, 2008. ADCOM 2008. 16th International Conference on*, dec. 2008, pp. 52 –57.

[18] S. Sethi and S. Udgata, "Imaodv: A reliable and multicast aodv protocol for manet," in *Wireless Communication and Sensor Networks (WCSN), 2009 Fifth IEEE Conference on*, dec. 2009, pp. 1 –6.

[19] V. Shah, H. Deng, and D. P. Agrawal, "Parallel cluster formation for secured communication in wireless ad hoc networks," in *IEEE International Conference on Networks*, vol. 2, 2004.

[20] A. K. Sunit Taneja and C. J. Hwang, "Secret key establishment for symmetric encryption over adhoc networks," 2011.

[21] P. Visu, W. Chembian, and S. Koteeswaran, "Security in multicast mobile adhoc networks," in *Advanced Computing, 2009. ICAC 2009. First International Conference on*, dec. 2009, pp. 38 –44.

[22] Wikipedia, "Latex — wikipedia, the free encyclopedia," 2012. [Online]. Available: http://en.wikipedia.org/w/index.php?title=LaTeX&oldid=413720397

[23] B. Wu, J. Wu, and Y. Dong, "An efficient group key management scheme for mobile ad hoc networks," *Int. J. Secur. Netw.*, vol. 4, no. 1/2, pp. 125–134, Feb. 2009. [Online]. Available: http://dx.doi.org/10.1504/IJSN.2009.023431