Security Problems in Heterogeneous Networks

Vinaykumar Muralidharan
Electrical Engineering
and Computer Science
The University of Kansas
Lawrence, Kansas-66046
Email: vinaym@ittc.ku.edu

Dr. Weichao Wang
Electrical Engineering
and Computer Science
The University of Kansas
Lawrence, Kansas-66046
Email: weichaow@eecs.ku.edu

Dr. Alexander Wyglinski
Electrical Engineering
and Computer Science
The University of Kansas
Lawrence, Kansas-66046
Email: alexw@ittc.ku.edu

***Abstract*— Security is a concern in the next generation Hybrid networks. This paper analyzes the various architectures that are proposed for next generation networks. Then we analyze their performance towards defending themselves from various malicious attacks and how the malicious nodes can exploit the differences in nature of the network to perform attacks. The solution to these attacks are provided by securing the network with a generic authentication mechanism that has a global vision, in avoiding the attacks that can bring down the entire network.**

The authentication mechanism follows a EAP based authentication that will decide on the type on authentication mechanism that is followed inside a particular cell. The base stations connected to each other through the MSC will follow a unified authentication mechanism. The solution is then simulated in NS-2 and results are analyzed.

I. Key Terms

Authentication, Network Security, Ad Hoc Networks, EAP, Credentials, Identity Verification, MCN-Multihop Cellular Network, BAAR - Base Assisted Ad-Hoc Routing, MSC-Mobile Switching Center.

II. Introduction

Next Generation wireless networks that are being developed are Hybrid Networks of different devices. The Fourth Generation Cellular Systems are design to accommodate users who can access the network in different modes. These devices have to be integrated on to the network through a secure enough infrastructure to make them communicate without any hassles. Since Ad-hoc networks are best effort networks they do not provide a guaranteed service, to obtain a network that can provide guaranteed service these networks are integrated with an underlying infrastructure say cellular networks. The backbone network will take care of managing the network and each device in the network will be directly connected to the Base station of that particular cell of the corresponding backbone.

In addition to the development of broadband physical layers, next generation wireless systems are expected to reuse the spectrum better. The recent attempts at throughput enhancement in traditional cellular networks include multi-hop cellular network **(MCN)**, integrated cellular and ad-hoc relaying system *(iCAR)*, hybrid wireless network *(HWN)* architecture, self-organizing packet radio networks with overlay **(SOPRANO)**, multi-power architecture for cellular networks **(MUPAC)**, and throughput enhancement wireless in local loop **(TWiLL)**, of which iCAR, SOPRANO, and TWiLL have direct support for real time traffic. The basic ingredients o these networks are throughput enhancements attempts has been the introduction of ad hoc network characteristics. Reducing the power of transmission is one of the well known techniques to enhance the network throughput. The 3GPP standard has imparted a multihop relaying in the initial versions although it currently appears to have been excluded in order to clear the concerns of signaling overhead, complexity and to achieve a finalized standard. The 4th generation wireless networks will have ad-hoc relaying modes in which users can directly transmit without using the help of the base stations. Many problems may arise in such networks when the malicious nodes get in to it. The malicious nodes might bring down the network by playing many attacks like modification attacks, fabrication attacks, impersonation attacks and passive attacks. This paper provides a solution for such attacks and provides simulation results how the solution works better when malicious nodes are taken into picture.

When we consider a secure integration of heterogeneous network Dr. Wang and et.al [1] proposes three main considerations when a hybrid networks are considered. Firstly, *developing a generic security management protocol that can span the network clouds*. A generic security management protocol is needed in the heterogeneous networks. Only when the devices in the network start speaking the same language the routing protocol becomes effective in routing the packets. Secondly, *developing an efficient resource monitoring and planning mechanism*. The malicious nodes can make a DOS attack in the entire network, so each local network should monitor the packets in the local network to eliminate such attacks. Thirdly, *Creating techniques to defend against collusive attacks*. The malicious nodes may collude not only with the local network but also with the global network so some sort of mechanism should be made to get rid of such collusive attacks.

III. Proposed Approach

The cellular networks have their own authenticating stations to authenticate each node. But in 4th Generation networks since the nodes can operate in ad-hoc modes the malicious nodes can bring down the network if the nodes communicate

directly with out the background infrastructure. In such a case an authentication and encryption mechanism should be in place to revocate or eliminate these malicious nodes.

The approach considers MCN type architecture, in this architecture all MHs in a cell take part in the topology discovery wherein each MH regularly sends to the BS information about the beacon power received from its neighbors. This information is used by the BS to estimate distances between MHs. For best-effort communication, all the calls share a single data channel and a single control channel. An on demand approach is used in the routing protocol. When a source A has a packet to send to the destination B to which a path is not known, it sends a Route request packet to the base station over the control channel. The BS responds with a Route reply packet containing the route, which is sent back to node A over the control channel. The route is computed using an Ad-Hoc Routing protocol approach. The source A upon the reception of Route reply packet transmits the data packet with the entire route information contained in it, to the next node on the path. The BS also chooses the data channel on which the transmission can take place.

The routing protocol implemented uses an Enhanced Authentication Protocol (EAP) authentication mechanism where the Supplicant negotiates with the type of security protocol to be used using EAP Protocol. Then it provides credentials using the agreed Security mechanism to the BS or undergoing the authentication phase. Then the BS of the Source and Destination negotiates the Session keys to be used to encrypt data. Here each device in the hybrid network is connected to a corresponding BS within its reach and the BS's uses their own authentication mechanism to reach its neighboring BS's. The EAP protocol is used within the cell to identify the security mechanism that is used within the cell. If the BS of the sender is different from that of the receiver the source might agree on its own security protocol and the receiver may agree on a different protocol. The BS will make the changes in transmission of the packets in such a network.

The diagram shows the basic operation of the network where in each node will have their own transmission range and they multi-hop with the neighboring nodes to reach to the BS. The BS uses their Backbone ring to communicate to the BS of the Destination which then multi-hops to the destination node. The use of such multi-hops increases the capacity to achieve the maximum capacity by utilizing the spectrum efficiently.

When the Source transmits the BS(S) its credentials the Receiver it wants to communicate to and the EAP it can use, the BS(S) will check for the receiver's location and if the BS(D) is different from the source the BS(D) will communicate to the D node and will identify the security mechanism it can support. Then the route is established. The packets will now be transferred to the destination with corresponding EAP's.

The following topics explain about the concept of basic authentication process, design of the routing protocol, simulation considerations, discussion of results, Security analysis and future work.

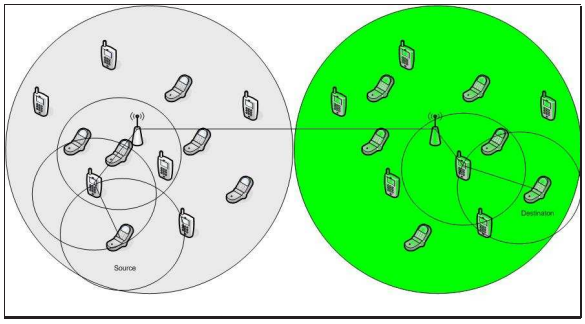

Fig. 1. Routing Protocol implementation

A. Generic Authentication Process

A generic authentication process has six major phases as shown in the figure below. Bootstrapping is the first phase, where a supplicant is securely provided, either offline or online, with something that it should have (a key) or something that it should know (a password) those authenticators would trust as a proof of the supplicant's eligibility to access protected resources or offer service. Once the bootstrapping phase is completed, the supplicant is ready to participate in the network. The pre- authentication process is where a supplicant presents its credentials to an authenticator in an attempt to prove its eligibility to access protected resources or offer services. Once the supplicant's credentials are verified, a credential establishment process is invoked to establish the supplicant's new credentials, which it will use as a proof of its identity and as a verification of its authorized state thereafter.

A credential could be a symmetric key, a public/private key pair, a commitment of a hash key chain, or some contextual information. The established credentials might be tagged with an expiry date after which the supplicant has to re-negotiate a new "certificate" of credentials. Upon success of all of the steps above, a supplicant is considered authenticated, which means that it is authorized to access resources protected by the authenticator. Within the authentication state, all Communication between the supplicant and the authenticator is authenticated by the source and validated at the destination using the established credentials. While authenticated, a supplicant's behavior is monitored for fear of its being compromised or misbehaving. A compromised supplicant may get its credentials revoked or its re-establishment of credentials request denied when its credentials expire. In both cases, the supplicant is isolated from the network. In this paper, we will focus on node-to-node authentication.

B. Node Authentication Phase

The state diagram in figure 2 represents possible states of a supplicant during the authentication process. The first state initializes the supplicant. In this state, the supplicant is usually supplied with necessary tools to carry on an authentication function. These tools could be supported authentication protocols (e.g., TESLA, 802.1x), authentication credentials (e.g., signed certificates), or identities of trusted entities. At the end

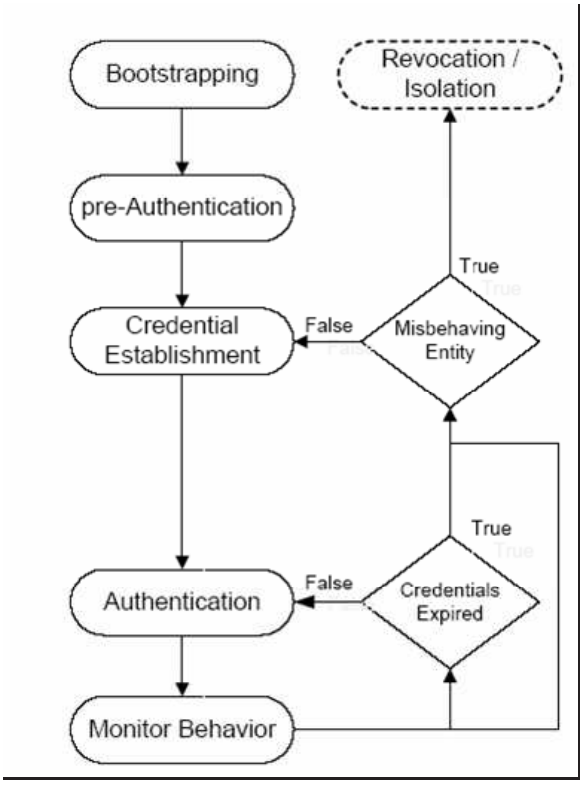

Fig. 2. Generic Authentication Process

of the initialization state, a supplicant has all necessary tools to authenticate to an authenticator.

Once a supplicant is initialized, it is ready to move on to the next state, which is discovery. During the discovery state, a supplicant scans for reachable services of interest. Each available service is expected to advertise its presence and list service-access requirements. A reachable service is one that is capable of directly making the supplicant aware of its presence (e.g., through periodic advertisements). At the end of the discovery state, a supplicant has a list of reachable services and the service-access requirements for each.

The following state is the selection state. Based on the list of reachable services and the service-access requirements of each, a supplicant filters accessible services of interest. The supplicant matches the tools it was supplied with during the initialization state to the service-access requirements advertised by each service. If none of the services match, the supplicant goes back to the discovery state. At the end of the selection state, a supplicant has a list of matching accessible services that are of interest to it.

The next state is the authenticating state. The supplicant uses the tools it was supplied with during the initialization state to attempt to authenticate to the authenticator. If the authentication process was successful, the supplicant moves to the authenticated state; if it fails the supplicant goes back to the discovery state. Within the authenticated state, the supplicant is considered trusted and is given appropriate access privileges to resources protected by the authenticator. The supplicant is bootstrapped with credentials that can be used to prove its access rights from there after.

Following the authenticated state, the supplicant frequently enters an evaluation state where its behavior is examined. Based on the outcome of the evaluation process the supplicant could either return back to the authenticated state (i.e. well behaving) or is put under probation (i.e. selfish or malicious). The probation state comes next, in which the supplicant enters as a penalty if it was determined to have behaved inappropriately. Eventually, the supplicant would be re-evaluated and given a chance to recover.

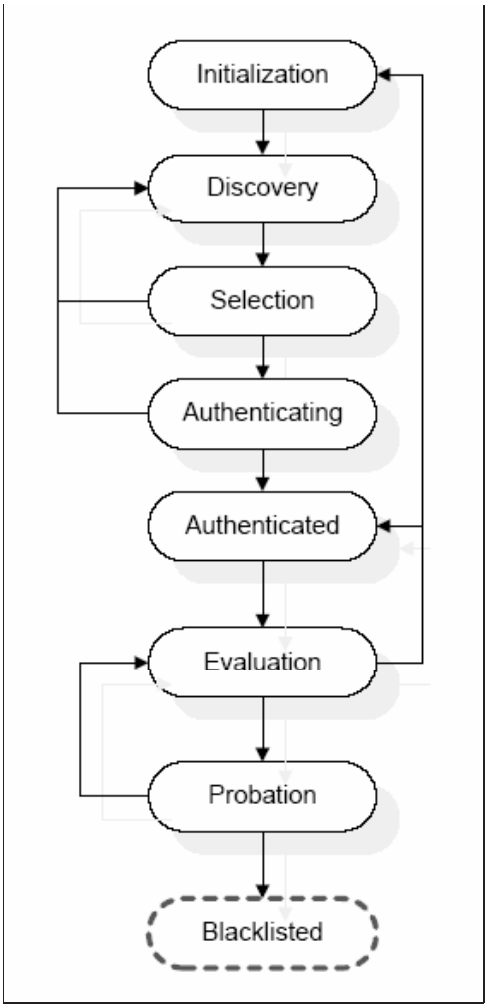

Fig. 3. Node Authentication

C. Design of Routing Protocol

The Routing protocol used is similar to BAAR (Base Station Assisted Ad-Hoc Routing) protocol. The protocol is implemented by integrating the EAP with BAAR protocol shown in figure . The source agrees with the Base station on the authentication mechanism using the EAP protocol and transmits to the BS on RACH (Random Access Channel) for establishing a connection to the network. The authentication server present in the BS authenticates the node. [3], Upon

getting authenticated the node will send a request on the destination it wants to communicate if the destination is present within the cell which is checked by the BS using its HLR and VLR then obtains a route on demand. Then the route is sent to the source. If the Destination is present in the same cell the packet is directly encrypted and transmitted in ad-hoc mode. If the Destination node is outside the cell the packet is transmitted to the BS which transmits to the BS (D) through the MSC. Then the BS (D) multihops it to the destination node.[4]

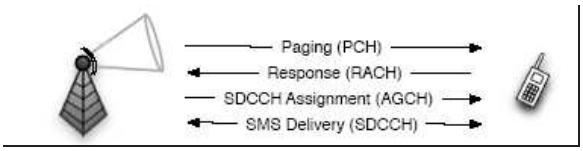

Fig. 4. Channel Access Method

The design of such a protocol is shown in the block diagram below. The packets once reaching the base stations are verified for their genuineness and an end to end authentication is made. Then the packets are transmitted to the BS (D). The BS (D) sends the packet through multihop to the receiver. The receiver decodes the data and sends an acknowledgement back to the source.

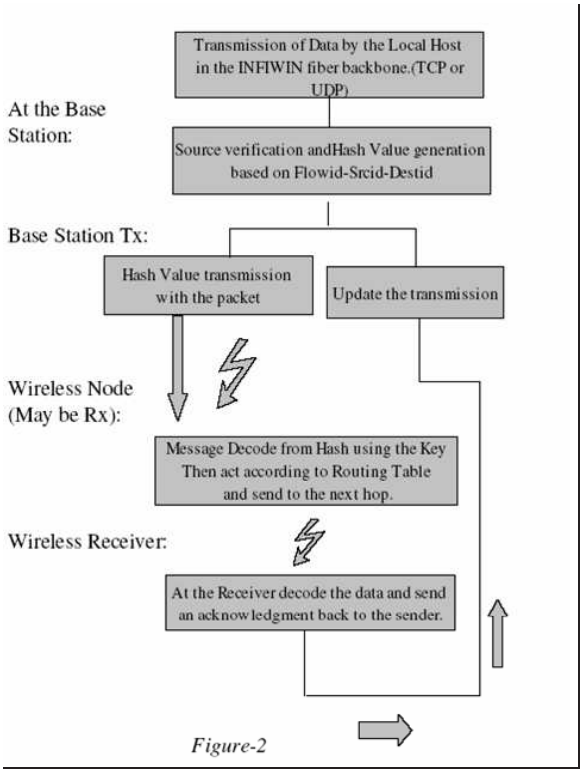

Fig. 5. Authentication Process used in the Protocol

IV. Simulations and Results

The simulations are made in NS-2.30, using the CMU wireless models. The network designed is across 2000 x 2000 m with the time of simulation for 100 to 300 Seconds. The wired LAN nodes considered are 8 nodes with 2 per BS. The Number of Base Station Trans/Receiver is 4 which are connected with a FIBER backbone. The wireless nodes generated are 300 which are positioned at random. 100 TCP/UDP connections are generated at random and are allowed to stay connected for the major amount of simulation times. The wireless physical layer is used which is simulated by CMU wireless labs. The MAC layer used is a modified 802.11 MAC layer. The heirarchical addressing helps to integrate wireless and wired nodes which follows the Domain.Cluster.Node pattern of generating the addresses. These addresses are generated using the NDP. The new wireless trace files for both nam and trace are generated, The connections, node coordinates and colors and alignment are generated as input scripts to the TCL files. Random Malicious nodes are generated of different properties. The properties considered are basically the nodes that might drop the packets or that might do a DOS attacks. Which are main properties of the malicious nodes.

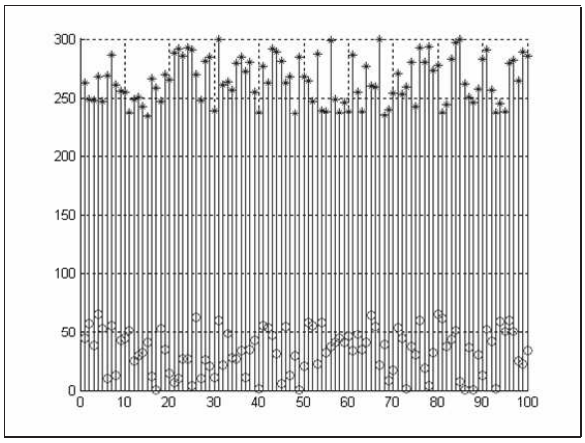

Fig. 6. Connection Pattern

The Routing Protocols used for multihopping are DSDV and AODV. Hierarchical Addressing is used for Wired-Wireless Integration. The simulation model is shown in the figure below.

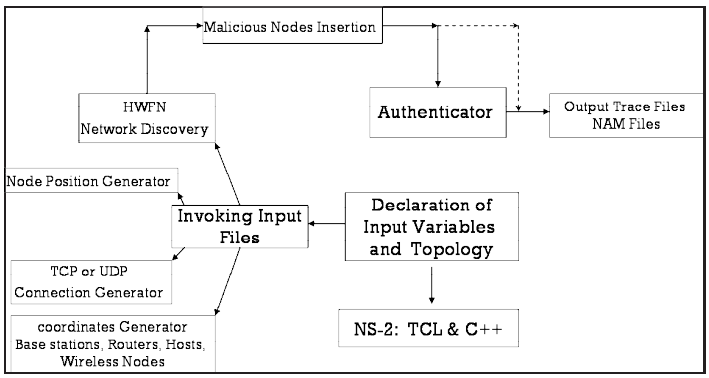

Fig. 7. Process Diagram of the Simulation

The simulations are done in NS-2 with input files being created from MATLAB 7.1. The NDP (Network discovery

Protocol) is written to split the network in to cells depending upon the positioning of the wireless nodes. The nodes then go through the NDP to enter the Authenticator which authenticates them. The malicious nodes are eliminated and after some time revocation process is initiated. Then the NDP provides the wireless nodes with the address which connects them to the network. The simulation model implemented is then analyzed with the authenticator in place and with out any authentication to work in pure ad-hoc mode and the trrace files is generated.

The trace files are then analyzed for throughput by analyzing the number of packets that are reaching the destination with and without the authenticator. The table below explains clearly that the authenticator in place increases the throughput of the system.

Number of Malicious Nodes	Simulation without Authentication R/S	Simulation With Authentication
5	0.9176	0.9614
10	0.8913	0.9574
20	0.8467	0.9354
30	0.7832	0.926
40	0.6743	0.9148

Fig. 8. Tabulation of Throughput

Since the malicious nodes are generated at random the seed in the generator is such that the nodes get generated in the middle of the network where the back bone is located. Hence when the number of malicious nodes increases we see a significant packet loss. If the malicious nodes are located at the farther end its impact will be much lesser than what we see in the above table. Also the authenticator increases the throughput significantly as the malicious nodes are eliminated from the system. The error we see in the authenticator is due to the use of wireless physical channel of the NS-2 simulation model which implements a default channel error model for dropping the packets. Hence we see that the Authenticated BAAR protocol will provide a high amount of throughput which is a necessary requirement for any service.

The graph above shows clearly the performance of the authenticator in the system to the degradation of the system due to the malicious node attacks without the authentication mechanism. We can see that the throughput increases as the number of dropped gets reduced. In the case of malicious nodes making TCP SYN attacks the authenticator in place reduces the throughput. Also the good put (The amount of correct transmissions without any retransmission) using the TCP connection increases. The communication overhead is more but is required for the safety of data transmission.

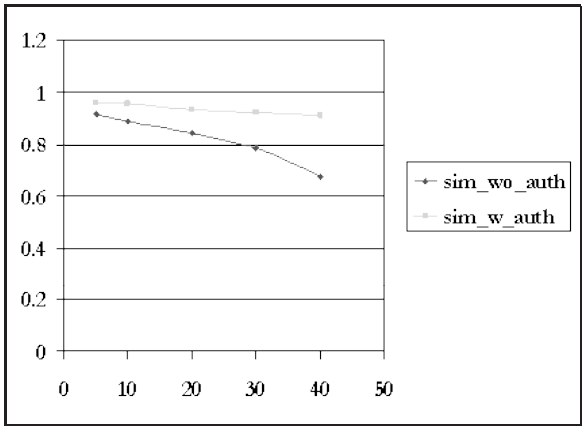

Fig. 9. Throughput Graph

V. SECURITY ANALYSIS

1. Blackhole detection: A malicious relayer can selectively drop packets received, instead of forwarding them towards their intended destination. This attack can potentially drop the throughput of a host to zero.Since BS keeps monitoring the entire cell region the malicious nodes that generates blackholes are kept under probation and isolated if necessary.

2. Impersonation Attacks: A host can try to impersonate other hosts in order to unfairly obtain free services or place blame for malicious actions on other hosts. Also a node can try to impersonate the base station to create havoc in the network. If a node tries to impersonate some other node the BS checks the credentials of both the nodes and their reputation and the malicious node is identified and further action is taken. This is taken care by the BS using the NDP and authentication server.[14]

3. DOS Attacks: Since each host has a direct cellular connection with the base station, any number of malicious colluding devices cannot prevent other hosts from receiving cellular service. Malicious hosts could however generate arbitrary amounts of useless traffic in the network, by generating requests for data that they do not intend to use, wasting network resources. The authenticator takes care of node to node authentication and eliminates the nodes which intend to do DOS. This is done by the use of beacon signal to estimate the channel use and the traffic generated.

4. Passive Attacks: Malicious nodes passively observe the traffic and gets important information to do an attack. These types of attacks are eliminated by using the session keys for encryption of the data by the EAP protocol.

5. Battery exhaustion Attacks: The malicious node change the routes to go to a particular node such that it gets exhausted. These types of attacks are prevented by integrating since the BS will not route all the packets towards the particular node and if a node generates such requests it will identify it to be a malicious node and isolates it from the network.

VI. Conclusion

In this paper we have proposed a secure integration for next generation 4G Hybrid wireless networks. We have also discussed about the various attacks that are possible and how the authentication mechanism can eliminate them for proper operation of the network. The proposed solution is simulated with NS-2 simulation environment, NS-2 is chosen as the simulation environment since it provides good tracefiles for the TCP connections that are being established which helps us to analyze the ouput obtained with great detail. The results are generated by implementing the above MCN architecture with EAP based authentication, which allows an EAP based authentication to provide a secure environment for data transmission. Since integration with cellular networks will provide a global vision for the nodes to speak a same language hybrid networks can reduce the malicious attacks with ease and since the network is already available less cost will require for modifying them to provide future networks. The authenticator defined for both single hop mode and multihop mode will eliminate DOS attacks even if the mobility of the malicious nodes are high since the nodes are integrated to the cellular network the malicious nodes cannot play around as it has to pass through the BS of the cell to get in to the network.

VII. Future Work

The future work includes creation of a Routing Protocol that uses path diversity based approach to reach to the nodes where connectivity is poor. The diversity scheme is generated by the protocol depending upon the channel quality and provides resilient networks. Reputation mechanisms should be implemented to reduce authentication overheads and speed up the routing process, This reputation ratings can be used for identification of malicious nodes with out any computations and the route selection process can be made by choosing nodes with high repuation rating. A Trusted Third Party (TTP) based authenication is also kept under consideration to improve the global awareness of the security mechanism that is being implemented.

References

[1] Joseph B. Evans,* Weichao Wang and Benjamin J. Ewy, *Wireless networking security: open issues in trust, management, interoperation and measurement*, The University of Kansas, KS 66045.

[2] Dimitrios Vogiatzis, Spyridon Vassilaras and Gregory S. Yovanof , *Secure Communication over Heterogeneous Networks with Clustered Mobile Ad hoc Extensions*, Athens Information Technology.

[3] Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta, *Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks*, Department of Computer Science and Engineering, The Pennsylvania State University.Mobicom-2006.

[4] Nidal Aboudagga1, Mohamed Tamer Refaei, Mohamed Eltoweissy,Luiz A. DaSilva, and Jean-Jacques Quisquater. *Authentication Protocols for Ad Hoc Networks: Taxonomy and Research Issues*.

[5] Asad Amir Pirzada and Chris McDonald, School of Computer Science and Software Engineering, *Kerberos Assisted Authentication in Mobile Ad-hoc Networks*, The University of Western Australia.

[6] B. Bhargava et al. *Integrating Heterogeneous Wireless Technologies:A Cellular Aided Mobile Ad Hoc Network (CAMA)*, Mobile Networks and Applications 9, 393408, 2004 Kluwer Academic Publishers.

[7] M. Danzeisen, et al., *Heterogeneous Network Establishment Assisted by Cellular Operators*, 5th IFIP TC6 Intl Conference on Mobile and Wireless Communication Networks, Singapore, October 2003.

[8] S. Vassilaras, D. Vogiatzis, G. Yovanof, *Misbehaviour Detection in Clustered Ad-hoc Networks with Central Control*, ITCC 2005, Las Vegas, USA, April 2005.

[9] L. Venkatraman and D. Agrawal, *A Novel Authentication Scheme for Ad Hoc Networks.* In IEEE Wireless Communications and Networking Conference (WCNC 2000), vol. 3, pp. 1268–1273, 2000.

[10] D. Park, C. Boyd, E. Dawson. *Classification of Authentication Protocols: A Practical Approach.* Proceedings of the Third International Workshop on Information Security.

[11] L. Zhou and Z.J. Haas, *Securing Ad Hoc Networks.* IEEE Network Journal, vol. 13, no. 6,1999, pp. 24-30.

[12] S. Gokhale and P. Dasgupta, *Distributed Authentication for Peer-to-Peer Networks*, In Symposium on Applications and the Internet Workshops 2003 (SAINT'03 Workshops).

[13] Bhatia, R., Li, L.E., Luo, H. and Ramjee, R. (2006) *ICAM: integrated cellular and ad-hoc multicast*, IEEE Transactions on Mobile Computing, Vol. 5, No. 8, pp. 10041015.

[14] Karlof, C. and Wagner, D. (2003) *Secure routing in wireless sensor networks: attacks and countermeasures*, Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, pp.113127.