International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.554 – 560

RESEARCH ARTICLE

Modeling of Empirical Approach to Ensure Secure and Efficient Data Forwarding in ADHOC Network

Rithesh Pakkala P.[1], J.V.Gorabal[2]

[1]Department of Computer Science & Engineering, Sahyadri College of Engineering & Management,
Mangaluru, Karnataka, India

[2]Associate Professor, Department of Computer Science & Engineering, Sahyadri College of Engineering & Management, Mangaluru, Karnataka, India

[1] rpakkala01@gmail.com , [2] jvgorabal@gmail.com

Abstract— Adhoc network is an assortment of wireless network which consists of number of wireless nodes in which interaction between the nodes does not follow the fixed infrastructure. End devices interact with each other when they are both within the same interaction range. Otherwise they depend on the neighbors to establish an interaction. Due to the natural behavior of the network, many of the anomalous activities easily take place in the network, which affects the security and efficient routing factors. Most of the research works in this field focused on either providing security or establish efficient interaction between the end devices in the network, but not both together. Hence it is most vital to propose a work to develop a model which provides both security and efficient communication in the adhoc network. In this paper, an empirical approach is proposed to design and implement the model which ensures secure and efficient data forwarding in the adhoc network. The proposed approach mainly concentrates on providing the data security services such as authentication, confidentiality and integrity in the model. Thereby anomalous activities such as packet dropping or packet modification attacks are easily handled. Also it establishes the more optimal and stable path from source to destination in which the transformed data is forwarded. Results show that proposed approach can achieve both data security and efficient data forwarding together in an intrinsic nature of the network.

Keywords— Adhoc Network, Anomalous Activities, Empirical Approach, Data Security, Efficient Data Forwarding

I. INTRODUCTION

Owing to their likely mobility and self-configuring feature, wireless networks are always favored. An ADHOC network is an assortment of wireless nodes equipped with both a wireless transmitter and a receiver that interact with each other via bidirectional wireless links either directly or indirectly. It does not require predetermined infrastructure. Each node may be proficient of acting as a router. Two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. In a single-hop network, all nodes within the same range communicate directly with each other. In a multi-hop network, nodes rely on other transitional nodes to broadcast if the destination node is out of their range.

Applications include virtual classrooms, military interactions, crisis seek and rescue operations, data possession in argumentative environments, communications set up in exhibitions, conferences and meetings, in battle fields among soldiers to coordinate defense or attack, at airport terminals for workers to share files etc.

The distinctive characteristics of Adhoc networks present a new set of challenges to security factor. The open network architecture, shared medium and remote distribution of network make it vulnerable to various types of attacks for instance packet dropping or packet modification attacks. Hence it is most imperative to propose security solutions for Adhoc network. The main aspiration of the security solutions is to ensure the security services such as confidentiality, integrity and availability (CIA) factors.

Another major hurdle in communication via adhoc networks is the efficient routing. Due to highly dynamic topology and mobility of nodes, makes the efficient routing is the taxing work in this field. Thereby there is a need to work to establish optimal path between the end nodes in the network and thus forward the data in the efficient and more stable route.

Most of the existing research works in this field focus on either providing security solutions or establishing the efficient routing in the network but not both. A new empirical approach has been proposed here to incorporate both security and efficient routing factors on AODV protocol in the adhoc network.

II. RELATED WORK

Most works on security of routing protocols have typically concentrated on the aspect of data forwarding, disregarding the facet of efficient routing. Also the solutions that target the efficient routing not consider the security issues. A number of techniques proposed for security and efficient routing.

Ahmed et al. [5] introduced a novel multi-copy routing protocol called Self Adaptive Utility based Routing Protocol (SAURP). SAURP is characterized by the ability of identifying potential opportunities for forwarding messages to their destinations via a novel utility function-based mechanism in which a suite of environment parameters such as wireless channel condition and encounter statistics are jointly considered.

Zhu et al. [6] proposed analytical energy efficient routing scheme PEER to track the energy consumptions due to various factors and to improve the performance during path discovery and in mobility scenarios.

Seung et al. [7] proposed a new routing technique called Security-Aware adhoc Routing (SAR) that incorporates security attributes as parameters into route finding. SAR enables the use of security as a flexible metric to improve the relevance of the routes discovered by the adhoc routing protocols. They developed a two tier classification of routing protocol security metrics and proposed a framework to measure and enforce security attributes on routing paths.

Stoleru et al. [8] presented Mobile Secure Neighbor Discovery (MSND), which offers a measure of protection against wormholes by allowing participating mobile nodes to securely determine if they are neighbors.

Kuo et al. [9] proposed a dynamic routing algorithm that could randomize delivery paths for data transmission. The algorithm is compatible with destination sequenced distance vector protocol without introducing extra control messages.

Zhu et al. [11] proposed a minimum energy routing scheme that consider the energy consumption for data packets as well as control packets.

Gomez et al. [13] introduced a power aware routing optimization (PARO) scheme that helps to minimize the transmission power needed to forward packets between wireless devices in adhoc networks. Using PARO, one or more intermediate nodes called “redirectors” elects to forward packets on behalf of source-destination pairs thus reducing the aggregate transmission power consumed by wireless devices.

Kang et al. [14] investigated the problem of energy-efficient broadcast routing over wireless static adhoc network where host mobility is not involved. They defined the lifetime of network as the duration of time until the first node failure due to battery depletion. They provided a globally optimal solution to the problem of maximizing a static network lifetime through a graph theoretic approach.

Rezaee et al. [15] proposed a cluster based routing protocol for mobile adhoc network. It uses clustering's structure to decrease average end to end delay and improve the average packet delivery ratio. In proposed method the routing is done quickly and its error tolerance increases due to the fact that routing is depended on the address of cluster heads. By failing any node in the route, its cluster head may use another node to forward packets.

Suanmali et al. [16] proposed selective acknowledgement (SACK) scheme, which can be easily attached on top of all source routing protocol. It discloses the malicious action and then recognizes compromised node or malicious nodes in the network.

From these observations, it is seen that security solutions should increase the packet delivery ratio and efficient routing scheme reduce the overhead during the route discovery. Therefore in this paper, a novel empirical approach is proposed to facilitate the ensuring of protection against packet modification attacks and finding of more optimal and stable data forwarding path between the end nodes while reducing the routing overheads and increasing packet delivery ratio.

III. PROBLEM DEFINITION

The proposed empirical approach is modeled to ensure secure and efficient data forwarding in ADHOC network, which is compatible with routing protocol AODV in order to protect against packet modification attack and establish the optimal and stable path between the end devices in the network which results in reduced routing overhead, increased packet delivery ratio and thus enhances the operational lifetime of the network.

IV. PROPOSED SCHEME DESCRIPTION

This section describes the proposed empirical approach in detail. The empirical approach is mainly consists of two major phases namely, data transformation and efficient data forwarding.

Fig. 1 shows architecture of the proposed system. The system consists of five modules namely, User interface (UI), Input, Control Processing, Testing/Maintenance module and Output module.

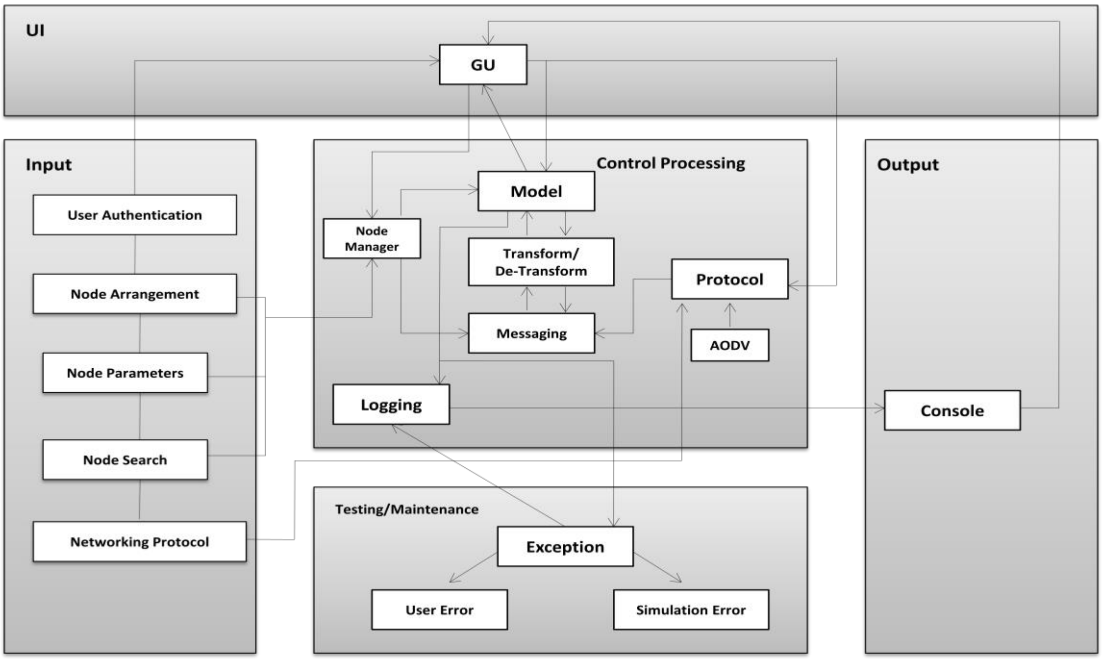

Fig. 1 Architecture of the Proposed System

The UI module contains the graphical user interfaces so that user can easily use the model.

In the input module, user has to authenticate in order to access the network resources so that authenticated user can configure the network. After the authentication, user creates the adhoc network by arranging the number of wireless nodes and initializing the node parameters such as, node name, node IP, position, power and cost. It also provides the node search feature so that user can search for a particular node in the network with its desired information.

In the control processing module, node manager is responsible for the node arrangements, parameter initialization and for the node search feature. User selects the two communicating end nodes among the network. Next user composes and transforms a message before forwarding. AODV protocol [2] is used to communicate between the two end nodes. Once the message is transformed, sender node sends the request message (RREQ) to the receiver. The receiver node may receive the requests from multiple paths. Receiver node selects the more optimal and stable path among the multiple paths and send the reply message (RREP) back to sender node in that path. On the reception of reply message, sender node forwards the transformed data in the efficient path. On the reception of transformed data, the receiver node de-transforms the data and verifies the data security services. All the routing details are logged and displayed in the console.

In the testing/ maintenance module, all the user errors and errors occurred during the simulation are handled.
All the simulation details are displayed in console of the output module.

A. *Data Transformation*

The data transformation phase deals with security aspects [3]. Fig. 2 shows the data transformation process and proceeds as follows:

1. The sender composes a message.
2. Apply the SHA-1 algorithm for the composed message and generates the 160 bits hash value.
3. Generate the sender's private key and public key using RSA algorithm.
4. The hash value generated in step - 2 is encrypted using RSA algorithm with sender's private key.
5. The result obtained in step - 4 is concatenated with the composed message in step - 1.
6. Finally, the concatenated result obtained in step-5 is encrypted using Triple-DES algorithm.

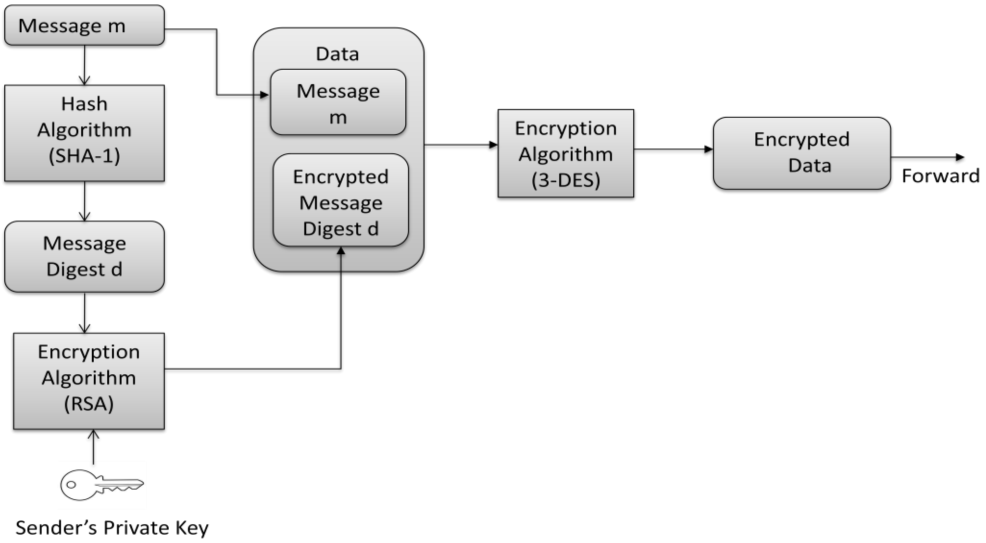

Fig. 2 Data Transformation Process before Forwarding

B. *Efficient Data Forwarding*

This phase mainly concentrates on forwarding the transformed data in the more optimal and stable path among the multiple paths in the network using AODV protocol. During the topology creation, the node parameters namely power and cost are initialized. After the data transformation, sender node sends the request message (RREQ) to the receiver node. Receiver node may receive the request on multiple paths in the network. On the reception of request, the receiver node chooses the optimal and stable path among the multiple paths based on the shortest distance between the nodes, minimum total cost of the nodes in the path and sends the reply message (RREP) in that path. The sender node then forwards the transformed data in the established efficient path.

C. *Data De-Transformation*

When the receiver node receives the transformed data, it follows the following procedure as shown in Fig. 3 to view the original message.

1. The receiver node decrypts the transformed data using Triple-DES algorithm.
2. The result obtained in step -1 after decryption is separated as message and encrypted hash value.
3. The encrypted hash value is decrypted using RSA algorithm with sender's public key.
4. For the separated message obtained in step-2, the new hash value of 160 bits is computed using SHA-1 algorithm.
5. Finally receiver node compares the new hash value generated in step-4 with the decrypted hash value obtained in step 3. If both the values are matches, then the receiver node concludes that message is authentic and views the message.

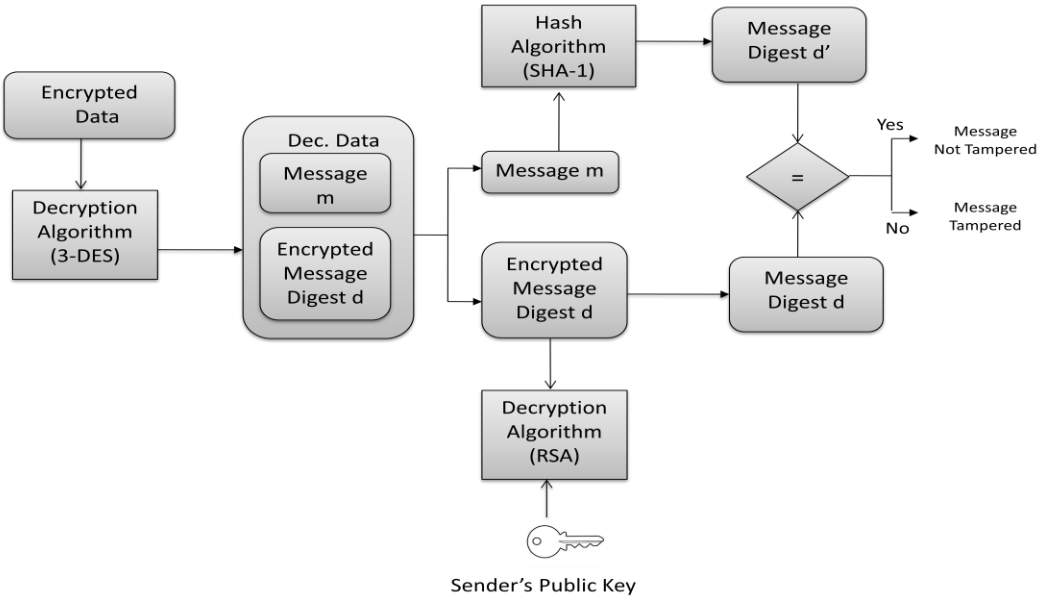

Fig. 3 Data De-Transformation Process after Receiver Node Receiving Transformed Data

V. PERFORMANCE EVALUATION

To test the performance of the proposed novel empirical approach, three test cases are considered in this paper.

Case 1: Number of nodes are considered six and all are initialized with power of 100 units. The node 192.168.10.1 is considered as the source node and the node 192.168.10.6 is the destination node. The result shows that the power consumption in each node using proposed empirical approach with AODV protocol is less as compared to AODV without empirical approach which is shown in Fig.4.

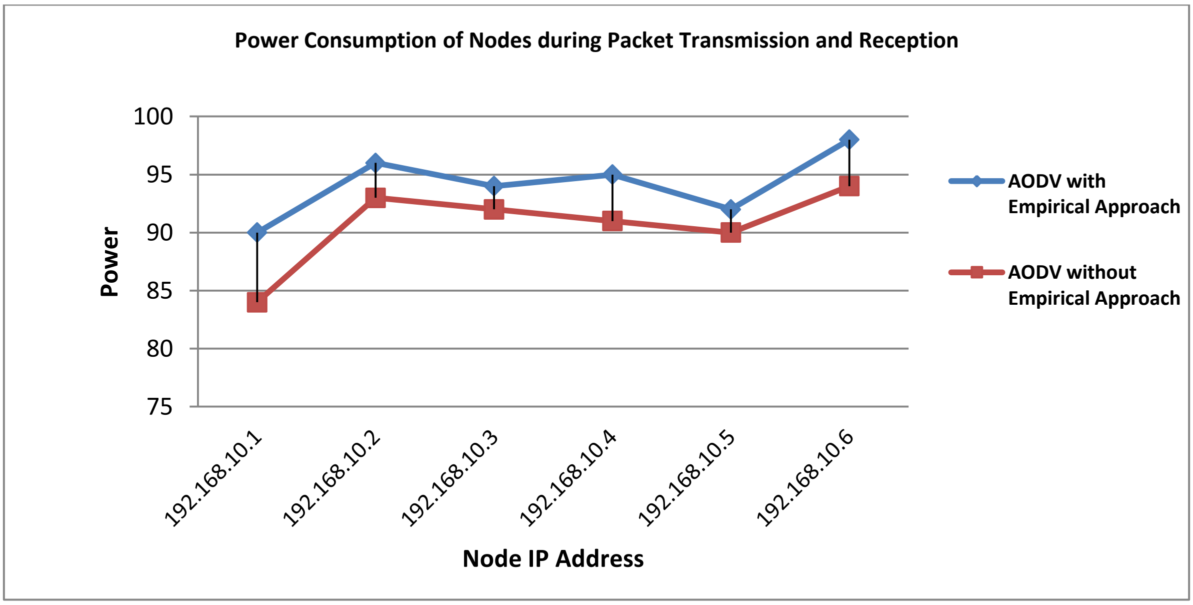

Fig. 4 Case – 1: Power Consumption of Nodes in the Network

Case 2: In case 2, malevolent nodes drop the packets that pass through it. The proposed empirical approach surpassed performance by 11% of AODV without empirical approach when there are 30% of malevolent nodes in the network. The end result shows that the packet delivery ratio is increased using proposed empirical approach with AODV protocol as compared to AODV without empirical approach which is shown in Fig.5.

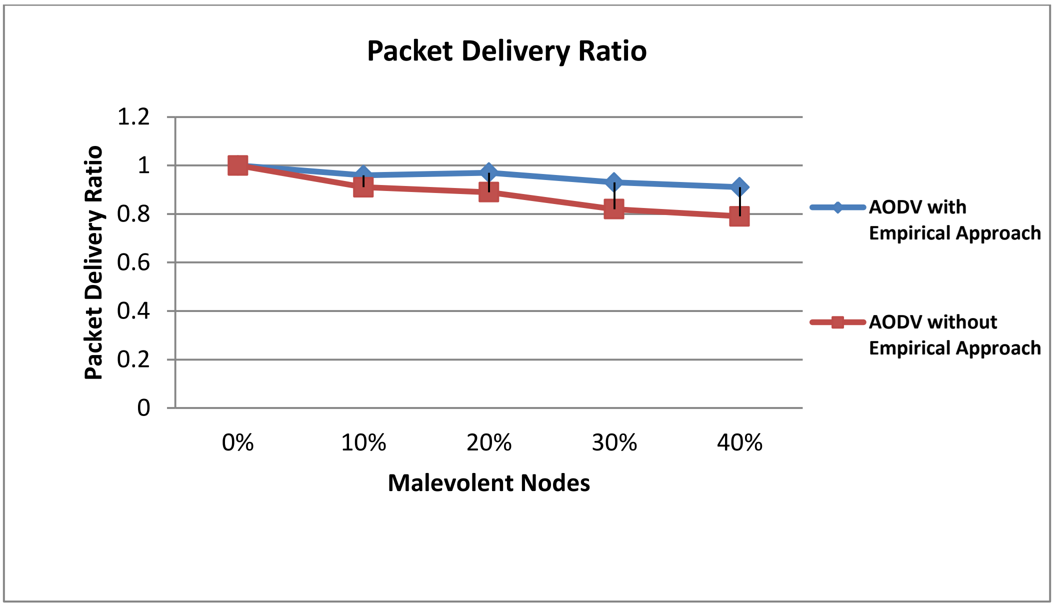

Fig. 5 Case – 2: Packet Delivery Ratio in the Network

Case 3: The proposed empirical approach maintains a less routing overhead compared to AODV without empirical approach which is shown in Fig. 6.

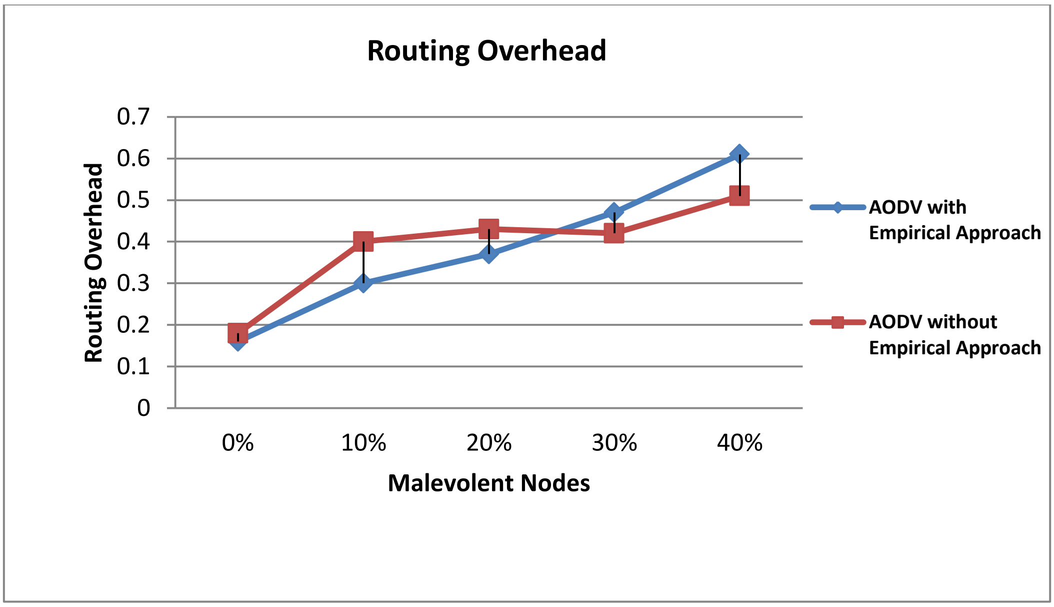

Fig. 6 Case – 3: Routing Overhead in the Network

VI. CONCLUSION AND FUTURE WORK

It is important to model a secure and efficient data forwarding protocol for adhoc networks due to its open medium and dynamic topology. The packet modification attack has always been a major threat to the security in adhoc network. In this paper, a novel empirical approach is proposed and incorporated on AODV protocol, which is specially modeled in order to tackle security attack namely packet modification and establishing efficient and stable route between the end devices using distance and cost factors to forward the data in the adhoc network. The results demonstrated constructive performances with respect to security, packet delivery ratio and end to end delay.

In the proposed approach, a novel cryptographic mechanism is incorporated to ensure the security of the data packets. It ensures the security services namely CIA factors. Although this mechanism generates more routing overheads, it can immensely improve the network's packet delivery ratio when the attackers are smart enough to forge the packets. In this paper we also discussed about the path discovery process using AODV protocol. It establishes an optimal and stable path between the end nodes based on distance and cost factors.

To augment the virtues of this work, the following issues can be investigated in the future work:

1. Possibilities of adopting different routing protocols other than AODV and evaluating the network performance.
2. Scrutinize the possibilities of adopting a key exchange mechanism to purge the necessity of pre-distributed keys.
3. Testing the performance of proposed novel Empirical approach in real network environment instead of simulation.

REFERENCES

[1] Dharam Vir, Dr. S.K.Agarwal, Dr. S.A.Imam , *"Investigation on Aspects of Power Consumption in Routing Protocols of MANET using Energy Traffic Model*" in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 1, January 2013.

[2] C. Siva Ram Murthy and B.S.Manoj, "*ADHOC Wireless Networks: Architectures and Protocols*", Pearson Publication.

[3] William Stallings, "*Network Security Essentials: Applications and Standards*", Fourth Edition.

[4] Elhadi M Shakshki, Senior member, IEEE, Nan Kang and Tarek R Sheltani, Member IEEE, " *EAACK – A Secure Intrusion Detection System for MANETs* " in IEEE Transactions on Industrial Electronics, Vol.60, No.3, March 2013.

[5] Ahmed Elwhishi, Pin-Han Ho, K. Naik, and Basem Shihada, "*Self Adaptive Contention Aware Routing Protocol for Intermittently Connected Mobile Networks*" in IEEE Transactions On Parallel And Distributed Systems ,Vol:24 , No:7 , 2013.

[6] J.Zhu, C.Qiao and X. Wang, IEEE Member, "*Model and Protocol for Energy Efficient Routing over Mobile Adhoc Networks*".

[7] Seung Yi, Prasad Naldurg, Robin Kravets, "*A Security-Aware Routing Protocol for Wireless AdHoc Networks*".

[8] R. Stoleru, H. Wu, H. Chenji ,"*Secure Neighbor Discovery in Mobile AdHoc Networks*" in Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, 2011.

[9] J Chin-Fu Kuo, Member, IEEE, Ai-Chun Pang, Member, IEEE, and Sheng-Kun Chan, "*Dynamic Routing with Security Considerations"*, in IEEE Transactions On Parallel And Distributed Systems, Vol. 20, No. 1, January 2009.

[10] J.Zhu, C.Qiao and X. Wang, "*PEER: A Progessive Energy Efficient Routing Protocol for Wireless AdHoc Networks*", INFOCOM'05, Mar.2005.

[11] J.Zhu, C.Qiao and X. Wang, "*A Comprehensive Minimum Energy Routing Protocol for Wireless AdHoc Networks*", INFOCOM'04, Mar.2004.

[12] S. Banerjee and A. Misra, "*Minimum Energy Paths for Reliable Communication in Multi hop Wireless networks*", MOBIHOC'02, June 2002.

[13] J. Gomez, A.T.Campbell, M.Naghshineh and C. Bisdikian, "*Conserving Transmission Power in Wireless AdHoc Networks*", IEEE Conference on Network Protocols, Nov.2001.

[14] Intae Kang and Radha Poovendran, "*Maximizing Static Network Lifetime of Wireless Broadcast Adhoc Networks*".

[15] M.Rezaee, M.Yaghmaee, "*Cluster based Routing Protocol for Mobile Adhoc Networks*".

[16] Nimitr Suanmali, Kamalrulnizam Abu Bakar and Suardinata "*Selective Acknowledgement Schme to Mitigate Routing Misbehavior in Mobile AdHoc Network*" in IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011.