SecAODV: Lightweight Authentication for AODV Protocol

J.A.D.C. Anuradha Jayakody
Faculty of Statistics and Computer Science, Faculty of Science, University of Peradeniya, Sri Lanka

Rohan Samarasinghe
Faculty of Computing, Sri Lanka Institute of Information Technology, New Kandy Road , Malabe, Sri Lanka

Saluka R. Kodituwakku
Department of Statistic s and Computer Science, Faculty of Science, University of Peradeniya, Sri Lanka

ABSTRACT
In nature of the transmission medium the broadcast, Wireless sensor networks are vulnerable to security attacks. The nodes are placed in a hostile or dangerous environment where they are not tangibly safe in the MANETs. In many application, the data obtained from the sensing nodes need a false, or malicious node could intercept private information or could send false messages to nodes in the network. Among the major attacks Eavesdropping, Spoof Attack, Denial of Service, Wormhole attack, Sinkhole attack, Sybil attack, Selective Forwarding attack, Passive information gathering, Node capturing, and False or malicious node, Hello flood attack are common. In this paper, authors have proposed and implemented an efficient light weighted authentication secure routing protocol on top of an AODV. The focused area of the proposed routing protocol is increasing the network security of the MANET. Additionally, the paper evaluates the implemented protocol using NS2 simulator in different networks with SecAODV.

General Terms
MANET, SecAODV, Light Weight Authentication, QoS, Security, Power Consumption

Keywords
MANET, SecAODV, Light Weight Authentication, QoS

1. INTRODUCTION
Wireless Sensor Network (WSN) or Mobile Ad-Hoc Network (MANET) provides wireless communication with high degree node mobility without a fixed infrastructure and the union of nodes forms an arbitrary topology [1].

MANETs are suitable to support some specific applications such as military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in exhibitions, conferences, and meetings, in battlefield among soldiers to coordinate defenses or attack, at airport terminals for workers to share files, etc.[1],[2],[3]. In ad-hoc networks, nodes can change position quite frequently. The nodes in an Ad-hoc network can be laptops, PDA, palmtops, etc. The identified challenges are often limited in resources such as CPU capacity, storage capacity, battery power, and bandwidth.According to the "Effect of Quality Parameters on Energy Efficient Routing authors, they stated that the each node participating in the network acts both router and a host and is willing to transfer packets to other nodes. For this purpose, a routing protocol [25] should minimize control traffic. The most commonly used Energy has become an important factor in MANETs. There is a limitation of battery life in an Ad-Hoc environment where the battery. The concept of power as one of the deciding factor in route selection can be crucial in route discovery and route repair phase [1],[2],[3].

Research on MANET Security Architecture Design" authors [16] have come up with security architecture for these networks by referring to the whole network. Referring OSI 7 layer model is built on each and every layer to consider an integral part of the network. The proposed Network Security Architecture consists of 5 layers namely, S0 Credible Infrastructure Layer, S1 Communication Security Layer, S2 Routing Security Layer, S3 Network Security Layer and S4 Application Security Layer. Using I-ADD process of security analysis, which is provided to prove a method for risk management solution, that used to analyzed on the characteristic, insecurity factor and security threats of these networks [23].

Authors in "Enhancing MANET Security using Secret Public Keys" [9] have mentioned about two types of authentication schemes as PKC – based and Identity – based authentication scheme. By considering the advantages and disadvantages of these two types they have used RSA as a basis for the cryptography scheme. Advantages of this scheme are speeding up the RSA encryption, verifying, and decryption and signing. They have proposed a secure solution to this network as four key securities where it hides the public keys and make them visible only to trusted nodes. This Key Management System considers four keys: - Identity Key, Public Key, Private Key and a Symmetric Key. Identity Key has known the information to anyone (e.g. Name). This paper proposed small Public Key for easy cryptography process, RSA Private Key to transfer only between trusted nodes. Asymmetric keys between each two nodes only for first-time communication.

"Secure Key Management and Verification of Mobile Ad Hoc Networks" [17] authors have provided secure key management and verification mechanism. They have considered the asymmetric key management combined with threshold cryptography. This paper has been used for formal specification of this network security properties, and key management is described using Z notation. Formalizing security and key management issue, the basic definition of the system were provided before which it is based on the definition of graph. They have observed Z check the effectiveness and powerfulness of their structure.

Authors in [18] "Authentication Algorithm to MANETs through Challenge – Response Based Architecture" which explains of providing Authentication through network layer using Challenge – Response based architecture. Authentication will be supplied using developed lightweight

authentication mechanism via a Challenge Response based protocol. They have provided Confidentiality and Integrity through symmetric cryptography; Hashing and key sharing achieve Diffie – Hell- man. They have implemented their mechanism, on a selected protocol called AODV. Which is for the nodes on the network they assigned a key. An extra field is added to packet structure called as Challenge which carries a challenge. This Authentication algorithm has embeds to node authentication to Route Discovery process through RREQ and RREP. The mechanism intercepts in the processes of sending Route Request (RRQ), receiving the RREQ, sending Route Reply (RREP) and receiving the RREP.

The above mentions are some of the researchers carried in the field of cryptosystem security in Wireless Sensor Networks. Author [19] "Alternative Authentication Scheme for Mobile Ad hoc Networks", which they have mentioned about Lightweight authentication, RSA, IBE, and PKC. They have proposed on to their future work to move on, how lightweight authentication scheme is provided with more lightweight implementation for a secret public key with less number of keys and less computational time.

Using the theories above utilized by the researchers and based on their future works they have mentioned, an improvement over the existing solution will be given by this research project which is a new solution for Wireless Sensor Networks.

2. RELATED WORK

This section discussed the general Security mechanisms and methodology proposed and implemented by researchers of past years. Due to the dynamic nature of the topologies consists characteristics of Wireless Sensor Networks such as dynamic topology, infrastructure less, node mobility, self-organizing, a shared medium, decentralized, arbitrary located mobile nodes it is hard to deploy and design a secure routing than the traditional network. It is a challenging task to address security issues in mobile ad-hoc network protocols.

Author [9] explained as there are internal attacks, which can be any legitimate participant of the routing protocol false in routing information and communication links and as well as external attacks are any other entity. In [10] authors have a classification of attacks based on Passive and Active attacks. Attacks which are difficult to detect since they do not involve in the attack but extract valuable information are called as Passive attacks. Eg: - Eavesdropping, Traffic monitoring, and analysis. Attacks that are performed by malicious nodes, which they are actively involved in the attack and does change done to information or system are called Active attacks. Eg: - Jamming, Man- in-the-Middle, Flooding attacks, etc. Authors on [11], [12] have explained the security of Wireless Sensor Networks, which can be divided into five OSI Layers which are Application layer, Transport layer, Network layer, Data link layer and Physical layer. This security architecture is designed based on the OSI Reference Layered model. In this type of wireless network different wireless users are available as Laptops, PDA, GSM, etc. Therefore, attacks in Application layer cannot define as a typical one since the application runs can differ.

There are many types of research carried since last two decades in the field of security, so to reduce the attacks and malicious nodes. The malicious attacks are present in all the layers of the security OSI, According to the Bing Wu, et.al under,"A Research on Survey of Attack and Countermeasures in Mobile Ad Hoc Networks" identified five layers. To achieve the security goals for Wireless Sensor Networks a new concept security mechanism implementation is looked forward to reducing discussed issues.

There are attacks which affect more than one layer which is called as Multi -layer attacks. Table 1 Summary classification of common attacks based on the security architecture and countermeasures proposed by other researchers.

3. PROBLEM IDENTIFICATION

In this research authors found a solution for the question "How to use a Cryptographic solution, to archive Authentication for data and as well as to users and how it can be applied to the current Cryptographic solution which is already implemented on AODV Wireless Sensor Networks."

WSN are much more vulnerable to attack than wired networks. The security issues are arrived in WSN due to a high level of vulnerability of wireless links, dynamic nature of the topologies, membership and roaming in a dangerous environment.

Table 1 Summary classification of common attacks based on the security

Security Level	Attacks	Countermeasures
Multi – Layer at- tacks	DOS Man – in – Middle	For these attacks, the safeguard can be the implementation of Security on different layer. Some protocols which help to avoid these problems are Aridane, SRP, ARAN, SAR, and SAODV [13].
Application Layer	Repudiation Data corruption	ARAN provides authentication and Nonrepudiation service using predetermined cryptographic Certificates for end – to – end authentication [12], [13].
Transport Layer	SYN Flooding attack Session hijacking	Implement SYN cookies in the three way shake. Author [12] explain the prevents against both these attacks, to implement Secure Socket Layer and Transport Layer Security protocol is to base in symmetric crypto algorithms.
Network Layer	Flooding attacks Black hole at- tacks Wormhole attacks	A cryptography – based solution pro-posed by author [14] for detecting and defending mechanism against this at- tack based on local broadcast keys. Author [15] explains in solving using packet leash, where information on packet to restrict the packet's maxi- mum to allow transmission distance. Some protocols prevent this attack such as Aridane, SRP, ARAN, SAR, and SAODV [13]. By monitoring on un- matched RREQ and put into blacklist.

Data link layer	Traffic monitoring and analysis Disruption on MAC	Traffic monitoring and analysis can be prevented by encryption on the data link layer. A detection algorithm pro- posed for this layer such as ERA-802.11 [15] and a secure Link Layer protocol such as LLSP.
Physical layer	Jamming / Impersonating Eavesdropping	Using of Spreading Spectrum or Code Spreading, Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spreading Spectrum (DSSS) [12].

4. MODERN SOLUTIONS

Security in Wireless Sensor Networks can be implemented using cryptosystem and as well as using on cryptosystem

4.1 Modern Cryptosystem Solutions

A modern cryptosystem is based on the key exchange mechanism. There are two types as Symmetric Cryptosystem only one key (need to share the key) and Asymmetric Cryptosystem use one pair of key (Private and Public keys). The user owns private Key whereas Public Key is public to everyone. Key establishment is done by an algorithm such as Diffie-Hellman algorithm [22].

4.2 Other Technologies

- Digital Signature – Based On Asymmetric Key (E.G. RSA). Each Node Needs To Have A Certificate Revocation List (CRL) of Revoked Certificates.

- Intrusion Detection System – Mostly For Fixed Wired Network so "Intrusion Detection in Wireless Ad Hoc Network" [13] Proposed A Design of Intrusion Detection and Response Mechanism for These Networks.

- Watch Dog And Path Rater – These Are Two Mechanisms To Improve Performance Of Wireless Sensor Network In The Presence Of Nodes Agree To Forward Packets : It Has been Modified Or Dropped As Unreliable Behavior Is Detected As Link Breaks.

Security in Wireless Sensor Networks can be implemented using cryptosystem as well as using on cryptosystem. In this research, security solution will be implemented using Modern Cryptosystem.

5. PROPOSED SOLUTION AND ALGORITHM

This novel implemented is top of the Route Discovery process of AODV. It shows how AODV Route Discovery and Route Maintenance process is explained as bellow.-

When a source node needs a route to a destination for which does not already have a path, it broadcasts a route request (RREQ)[24] packet through the network. Nodes are receiving this packet update their information for the source node and set up backward pointers to the node of origin in the route tables. In addition to the node of origin's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with a corresponding sequence number greater than or equal to which contained in the RREQ. If this is the case, it unicasts an RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive an RREQ, which they have already processed, they discard the RREQ and do not forward it. As the RREP is propagated back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives an RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically traveling from the source to the destination along that path[24]. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the unreachable destination(s)[24]. After receiving the RERR, if the node of origin still desires the route, it can reinitiate route discovery.

Algorithm

The developed Authentication algorithm runs on top of the Route Discovery Process. It intercepts in the processes of sending Route Request (RRQ), receiving the RREQ, sending Route Reply (RREP) and Receiving the RREP. Following fig 1 describes propose developed the algorithm.

```
Set key for node
Generate random string from the sequence number
IP address, Sequence Number, random string encrypted
Set the sequence number, random string in a table
Set the encrypted value into RREQ package
Broadcast it to nodes

//Receive the RREQ and Send RREP

if (receiver node knows the key)
        decrypt the encrypted value

        if(Sender IP address == decrypted field IP address)
                Node is trustworthy

                if ((sender IP address == decrypted field IP address) || ( Receiver node
                        know the path))
                        Generate hash value with Source IP address, Random String, key
                        to be send with the RREP
                else
                        broadcast the packet
        else
                drop the RREQ
else
        broadcast the packet


// Receive the RREP

if (Random string in RREP == Random sting in table)
        Generate hash value with source IP, Random string and the key
        if ( new hash value == send hash value)
                authenticated node
        else
                drop the packet
else
        drop the packet
```

Fig 1 Developed Authentication Algorithm

6. SIMULATION MODEL

Authentication algorithm was developed on NS2. The implementation on NS2 allows testing developed algorithm in various situations with a small to a large number of nodes. The Algorithm was written using C++ by modifying the existing AODV algorithm in NS2. Then the simulation environment has been created using the TCL script.

AODV in NS2 has been developed according to the AODV RFC [20], and like the RFC suggests, algorithm disables the use of hello packets by default. In order to run the Algorithm correctly it was needed to turn off hello packets, and therefore, authors left the default configurations as it is. If the

Hello packets are a must for any certain application that uses this Authentication Method, this research project suggest is to implement the same challenge based mechanism for Hello send and Hello Receive Methods as the RREQ send, and RREQ Receive Functions. In the TCL script, all the nodes are assigned with a key. In NS2, this research project has installed OpenSSL 1.0.0a [21] to Ubuntu machine to achieve AES Encryption and Decryption and HMAC function.

The algorithm has been developed mainly in the body.Cc file. This algorithm is implemented for the Route Discovery process of AODV protocol. It has been developed inside "AODV:sendRequest(sadder t dst)" function. Receiving a Route Request has been implemented inside "AODV:recvRequest (Packet *p)" part and Sending a Route Reply has been implemented inside void "AODV:sendReply" function. Finally Receiving a Route Reply has been implemented inside void "AODV:recvReply Packet *p)" function. These functions work as how they are described in the sections mentioned above. Several variables are defined in the "body.h" file that supports the implementation of the algorithm.

7. RESULTS AND DISCUSSION

The TCL Script is designed with the parameters as shown in Table 2. This is the test bed or test case this project considered when taking the results between the existing AODV and Authenticated AODV. Some nodes run this TCL Script as 5, 10, 20, 30, 40 and 50. In order to achieve Security, a password is assigned to each node as 123.

Table 2 Simulation Parameter of Existing Routing Protocols

Parameter	Value
Topology	1000mx1000m
Bandwidth	11Mbps
MAC Protocol	802.11
Number of Nodes	5, 10, 20, 30, 40, 50
Mobility Model	Propagation/Two Ray Ground
Antenna Type	Omni Antenna
Routing Protocol	AODV, Authenticated AODV
Queue Type	Queue/Drop Tail/ PriQueue
Simulation Time (s)	1000s
Traffic Type	CBR
Number of Connections	2
Connection Type	TCP/FTP
Password Assigned to Nodes	123

The graphs below have been generated to show the performance of new authenticated AODV with the General AODV. Graphs are generated to show Packet Delivery Ratio, Average end-to-end delay, and throughput of the network. TCL Scripts trace files and AWK Scripts have been used to gather and analyze the data from NS2 as described in the Methodology.

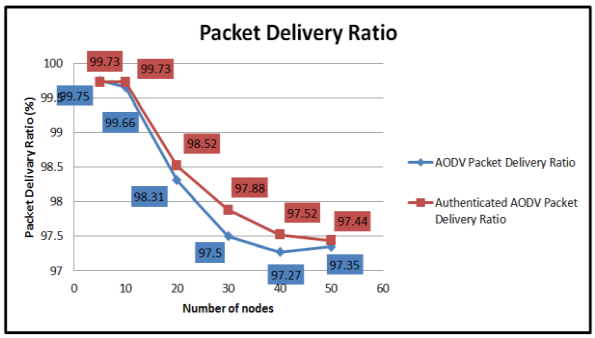

Fig 2.Packet Delivery Ratio between existing AODV and Authenticated AODV

The Packet Delivery Ratio between existing AODV and Authenticated AODV is important to note that when some nodes increase, Packet Delivery ratio is higher in Authenticated AODV rather than existing AODV(Fig 2). When referred to a research paper [18] it is clear that data communication starts after, only when nodes are properly authenticated. That means there is lesser chance of dropping or missing packets because of poor communication lines. Here reliability is also achieved, in this solution. So a high packet delivery ratio can be archived.

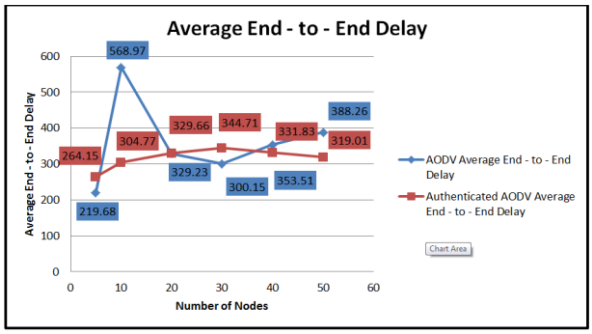

Fig 3 Average End - to - End Delay (ms) between Existing AODV and Authenticated AODV

Analysing Average End – to – End Delay between Authenticated AODV (Fig, 3) and existing AODV, It is quite hard to come to a conclusion about the Differences between Authenticated AODV and Existing AODV. However, according to the architecture of the Algorithm, since only general RREQ, and RREP packets are used, there is no additional overhead to the network, so only overhead to nodes that process packets. Therefore, this authenticated AODV; there is no effect of the delay on the network.

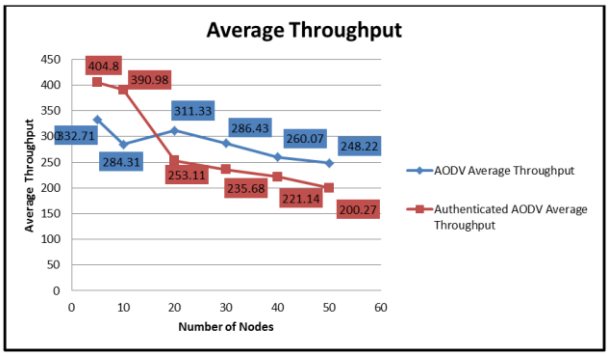

Fig 4 Between Existing AODV and Authenticated AODV] Average Throughput [kbps] between Existing AODV and Authenticated AODV

Throughput (Fig 4) is reduced in this authenticated AODV. This happens due to the process of the Authentication Algorithm, due to the encryption and decryption and as well as hashing process. It is less compared this shows, that it can be decided that the Authentication process, only adds a slight load to the General AODV algorithm.

7. CONCLUSIONS

The main intention of the research is to develop a framework for Wireless Sensor Networks to provide efficient, decentralized Security solutions such as Authentication and Integrity. Within the context of this research report has discussed the implementation of the Lightweight Authentication Algorithm to AODV to the routing process.

Selection of the AODV protocol has come through the conclusions obtained from the Protocol Analysis done. From the Analysis of Protocols, came to a Conclusion that the AODV Routing Protocol is the Best to Implement Security solutions. As also described in Analysis Section the main reason for this is its High Packet Delivery Ratio. Furthermore, AODV is a reactive Routing Protocol, which suits best for Wireless Sensor Networks environment because it only sends a small number of Routing Information only when needed unlike in Proactive Routing Protocols.

After deciding the Routing protocol, implemented the proposed authentication algorithm on top of AODV to secure the routing process. This implementation was done in NS2 Simulator. Results are obtained and considered the Packet Delivery Ratio, End - to – End Delay and Throughput for new solutions. According to the obtained results, came to the conclusion that the routing process can obtain sufficient authentication requirements through the developed algorithm. Furthermore with the use of other security implementations of the other authors in the research, authors have also been able to provide Authentication with integrity to further enhance the security in Wireless Sensor Networks.

8. ACKNOWLEDGMENT

This work has been supported by University of Peradeniya, Sri Lanka and Sri Lanka Institute of Information Technology, Malabe, Sri Lanka.

9. REFERENCES

[1] Elizabeth Royer and C-K Toh, “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks”, IEEE Personal Communications Magazine, April 1999, pp. 46-55.

[2] Priyanka Goyal, Vinti Parmar and Rahul Rishi,“ MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011: online

[3] M. Bouhorma, H. Bentaouit and A. Boudhir, "Performance comparison of ad-hoc routing protocols AODV and DSR," International Conference on Multimedia Computing and Systems, ICMCS '09, Pages511 - 514, 2009.

[4] Marwan Krunz and AlaaMuqattash,”A Power Control Scheme for MANETs with Improved Throughput and Energy Consumption.”

[5] Liang W., "Minimizing energy and maximizing network lifetime multicasting in wireless ad hoc networks," in IEEE International Conference on Communication (ICC2005), pp. 3375-3380, 2005

[6] Marwan Krunz, AlaaMuqattash, and Sung-JuLee, “Transmission Power Control in Wireless Ad Hoc Networks: Challenges, Solutions, and Open Issues.”

[7] Charles E. Perkins, ElizabethM. Belding-Royer, and Samir R. Das. Ad hoc On-Demand DistanceVector (AODV) Routing. RFC 3561, July 2003.

[8] Mehdi Barati , Kayvan Atefi, Farshad Khosravi and Yashar Azab Dafial ,”Performance Evaluation of Energy Consumption for AODV and DSR Routing Protocols in MANET”, 2012 International Conference on Computer & Information Science (ICCIS)

[9] C. Margi and K. Obraczka, “Instrumenting networking simulators for evaluating energy consumption in power-aware ad-hoc network protocols,” in International Symposium - MASCOTS’ 04, October 2004.

[10] S. Doshi, S. Bhandare, and T. X. Brown, "An on-demand minimum energy routing protocol for a wireless ad hoc network," ACMSIGMOBILE Mobile Computing and Communications Review, ACMUSA, Volume 6 Issue 3, July 2002.

[11] ZdravkoDanailov. Attacks on mobile ad hoc network. Sem- inaRarbeit. URL http://www.slideshare.net/xeon40/ attacks-on-mobile-ad-hoc-networks-12619703.

[12] Jie Wu MihaelaCardei Bing Wu, Jianmin Chen. A survey of attacks and coun- treasures in mobile ad hoc networks. Wireless/Mobile Network Security, 2006 Springer.

[13] Daya Gupta Jaspal Kumar, M. Kulkarni. Secure routing protocols in the ad-hoc network: A review. 2010 for International Conference [ICCT-2010], 2:8, December .

[14] C. Meadows P.Syverson L. W. Chang L. Lazos, R. Poovendran. Prevent- ing wormhole attack ad hoc networks: A graph theoretic approach. Wireless Communication and Networking Conference, 2005 IEEE.

[15] J. Tygar D.Song A.Perrig, R.Canetti. The Tesla broadcast authentication protocol. Internet Draft, 2000.

[16] Zhu Qing-Sheng Li Shi-Chang, Yang Hao-Lan. Research on manet security architecture design. 2010 International Conference on Signal Acquisition and Processing, 2010 IEEE.

[17] Zafar NA and Ahmed IC. Secure key management and verification of mobile ad hoc network. J A Sci 2013;9(1):117-123. ISSN: 1545-1003. URL http://www.jofamericanscience.org.

[18] B. Anushka S. Visagan-B. Hettiarachchi L. Rupasinghe, R. Tennekoon and P. Basnayake. Authentication algorithm to manets through challenge –re- response based architecture. PNCTM, 2, JAN 2013.

[19] MD ASRI NGADI TAMEEM EISSA, SHUKOR ABD RAZAK.Authentication scheme for mobile ad hoc networks. Faculty of Computer Science and Information Systems, UNIVERSITI TEKNOLOGI MALAYSIA SKU- DAI, JOHOR, MALAYSIA.

[20] RFC for AODV, Electronically Available on URL http://www.ietf.org/rfc/rfc3561.txt.Accessed on 02/02/2014

[21] The OpenSSL, Electronically Available on URL http://www.openssl.org/, Accessed on 02/02/2014

[22] P. C. van Oorschot and M. J. Wiener, On Diffie-Hellman Key Agreement with Short Exponents. EUROCRYPT'96, LNCS 1070, Springer-Verlag,1996, pp. 332–343.

[23] Li Shi-Chang. "Research on MANET Security Architecture Design", 2010 International Conference on Signal Acquisition and Processing, 02/2010

[24] International Journal of Soft Computing and Engineering .., [Available on URL] http://www.ijsce.org/attachments/File/Vol-1_Issue-4/D0103081411.pdf (accessed January 15, 2016).

[25] " Effect of Quality Parameters on Energy Efficient Routing ..." http://www.enggjournals.com/ijcse/doc/IJCSE11-03-07-166.pdf. N.p., n.d. Web. 15 Jan. 2016 <http://www.enggjournals.com/ijcse/doc/IJCSE11-03-07-166.pdf>.