T-AODV Heuristic based Trust implementation in Ad-hoc Routing Protocol for Wireless Sensor Networks

Shashika Lokuliyana
Department of Information Systems Engineering
Faculty of Computing, Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Lakmal Rupasinghe
Department of Information Systems Engineering
Faculty of Computing, Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

ABSTRACT

Wireless Sensor Networks (WSNs) operates with an open network topology without well-established infrastructure. Due to the absence of a centralized administration in network management, WSNs are highly vulnerable to various malicious attacks. The introductory of such a malicious node in a network may lead the network to security breaches, miscommunication, starvation and finally decay. In this paper, the authors attempt to reduce the vulnerability of a WSN node communicating with a malicious node by establishing a TRUST based authentication and filtering routing mechanism. The authors aim to detect and prevent potential attacks such as DoS attacks and Blackhole attacks, thus providing the associated security needed in order to build up relationships among each other to communicate.

The authors have used the existing AODV routing protocol and modified to perform a heuristic based TRUST metric calculation. In a situation of a suspected malicious node, the TRUST based security protocol detects and isolate the attacker as the communication channels proceed. The TRUST based AODV protocol has been implemented and evaluated with the NS-2 simulator and simulation results are compared with the existing protocols.

General Terms

Security Protocol, Algorithm, Framework

Keywords

WSN, AODV, TRUST, Security Protocol

1. INTRODUCTION

Wireless Sensor Networks has experienced an exponential grows in the past decade because of the ubiquitous nature of its implementation. The autonomous nodes communicate in a decentralized format with an unrestricted mobility due to the absence of the underlying infrastructure. Significant applications of WSNs include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks that cannot rely on centralized and organized connectivity.

Network topology changes are unpredictable due to the dynamic mobility of the mobile nodes. This topology changes makes it more complex to implement currently existing security implementations because of the absence of a centralized infrastructure. Today's networking relays on fixed infrastructure to manage and provide security. With the absence of the centralized infrastructure the establishment and management of the communicating nodes becomes more complex.

Due to mobile device configurations, ad-hoc networks are generally more prone to physical security threats. Because of the misconfigurations the possibility of eavesdropping, spoofing, denial-of-service, and impersonating attacks has also increased [3]. Similar to fixed networks, security of the Ad-hoc networks are considered from the attributes such as availability, confidentiality, integrity, authentication, non-repudiation, access control and usage control. New threats, such as attacks arising from internal malicious nodes are heard to define, due to the salient characteristics of Ad-hoc networks [4]. Table 1. provides summary on security issues in ad-hoc network nodes related to TCP/IP layered stack.

Table 1. Security issues related to each layer in protocol stack [11]

Layer	Security Issues
Application	Prevention, detection of viruses, worms, malicious nodes, application abuse
Transport	Authentication and end to end data security through encryption techniques
Network	Security of Ad-hoc routing protocols and associated parameters
Physical	Preventing signal jamming, denial of service attacks and other active attacks

2. LITERATURE REVIEW

Based on the routing information update mechanism, routing protocols in wireless ad-hoc networks can be classified into three types as reactive protocol (on demand), proactive protocol (table driven) and hybrid protocol [5].

On demand protocols such as AODV [5], DSR [6], SAODV [7] and SAR [8] discover the route once needed. Whereas table driven protocols such as OLSR [9] and DSDV [10] will keep network topology information and change routing information periodically. This periodical updating causes a flooding of active route requests, in which increase the overhead inside the network. Hybrid protocols are a combination of proactive and reactive protocols, where the nodes choose the best way in communication and establishment.

The reactive protocols display considerable bandwidth and overhead advantages over proactive protocols because of the high overhead proactive protocols create. Among them AODV routing protocol offers quick adaption to dynamic link conditions, low processing, low memory overheads and low network utilization.

The standard AODV routing protocol assume that there are no malicious nodes participating in routing operations. This assumption cannot be applied in WSNs because of high mobility, de-central coordination mechanism, open network and collaborative communication between nodes, which makes WSNs more vulnerable to attacks.

There are two mainstreams to enhance the security aspect in AODV routing protocol i.e. cryptographic mechanism and trust based mechanism.

Cryptographic mechanism guarantees the confidentiality and integrity aspects of routing, while protecting the exchanged packet data, route creation, and route maintenance during communication. Some of the proposed solutions are Secured AODV (SAODV) [7] by Zapta, introducing security based on public key cryptography. The assumption is that every node has certified public keys of all network nodes and also SAODV requires heavy weighted asymmetric cryptographic operations because signature generation and signature validation.

A solution was proposed by Cerri and Ghioni as A-SOADV [12] which uses an adaptive mechanism, where nodes reply if they are not overloaded.

Eichel and Roman proposed AODV-SEC [13] which is an improved version of SAODV using a new certificate with a certifying authority (CA). CA should be centralized for every node in the network. Which in hence breaks the first rule of MANET defining no centralized management.

Pirzada et al. proposed a new pragmatic method for establishing trustworthy routes in AODV [14]. An agent is used to populate the trust reputation in each node to every other node making the scenario a semi-centralized environment. Based on this Pushpa [15] developed a trust mechanism where complex trust factor calculation is introduced via node trust and route trust.

Zhe et al. [16] proposed an AODV routing protocol based on credence model but need more space memory to save the credence value of each neighbor. Where Griffiths et al. [17] proposed STAODV, a trust model using acknowledgments as an observing factor.

Kurosawa et al. [18] proposed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals.

The significance of all the trust developments is that the proposed mechanisms are adopted only in centralized or semi-centralized environments and uses only one observing behavioral factor of the node.

The solution is Trust based mechanism with the advantages;

- No need of requesting or verifying certificates all the time
- Unnecessary to add any signature or cryptography methods, in the message packets, making low overhead.

The authors are going to improve the security of AODV routing protocol with trust mechanism method to keep the performance.

3. PROPOSED TRUST MECHANISM

The author has performed some modifications to the existing AODV protocol by adding trust level calculation. Where the proposed mechanism is able to detect and prevent the attack by isolating the detected node.

3.1 Trust Factors

In order to build up the trust matric the behavior of a mobile node is taken into account and thus a matric is developed to measure the trust value. The behavioral factors mentioned below were taken in to account,

1. Packet Delivery Ratio(PDR)
2. Basic Secure Location
3. Node Motion

3.1.1 Packet Delivery Ratio (PDR)

This is defined as the ratio of the number of packets received by the destinations to those sent by the sources. To perform the trust calculation, each node should collect all the activity information from its neighbor nodes. Each node will detect the anomaly in its neighbor node based on the calculation of the activities packet in nodes. Trust calculation performs when the node begin communication process. Each node will hear and calculate the total of received and forwarded route request-RREQ, route reply-RREP, route error-RERR, AODV control packets and CBR data packet.

$$PR_{aodv}=\text{AODV control packets received to node} \quad (1)$$

$$PT_{aodv}=\text{AODV control packets transmitted from node} \quad (2)$$

$$PR_{cbr}=\text{Data packets received to node} \quad (3)$$

$$PT_{cbr}=\text{Data packets transmitted from node} \quad (4)$$

$$PDR_{aodv}= \frac{\sum PR_{aodv}}{\sum PT_{aodv}} \quad (5)$$

$$PDR_{cbr}= \frac{\sum PR_{cbr}}{\sum PT_{cbr}} \quad (6)$$

3.1.2 Basic Secure Location

The position of the destination node with respect to the positioning of the source node is taken into consideration. There are two level of positioning index valued provided be the source node, according to the x and y coordinates of the destination node referring to Figure 1 given below.

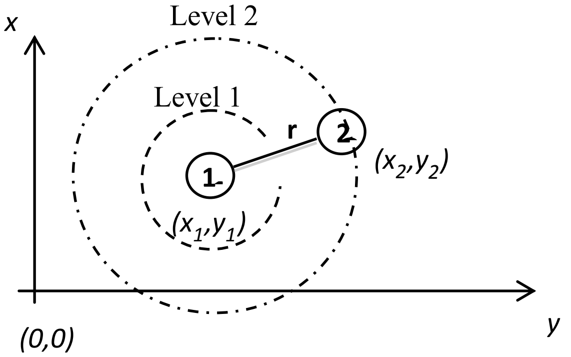

Figure 1: Distance between two nodes: Node 1 and Node 2

The radius between the two nodes can be calculated by,

$$r= \sqrt{(\Delta x)^2+ (\Delta y)^2} \quad (7)$$

Where,

$$\Delta x = abs|\, x_2 - x_1| \tag{8}$$

$$\Delta y = abs|y_2 - y_1| \tag{9}$$

After calculating the radius, it is being checked whether the destination done (node 2) resides within the levels defined by the source node (node 1). This levels of trust, is pre-defined and normally should be tuned according to the environmental situations.

The positioning factor (P_r) will be defined following algorithm,

```
if r ≤ Level 1
    $P_r$=1.0     //since the two nodes are near each other the trust index is high
else if Level 1<r   &&  r ≥ Level 2
    $P_r$=0.5     //trust to an certain extend
else if Level 2<r
    $P_r$=0.0     //not trusted
```

3.1.3 Node Motion

In an Ad hoc environment the nodes are randomly moving, with different velocities and in different directions. The proposed solution takes in to account of this random movement of nodes with respect to each other to provide a movement factor in the trust calculation process.

The random generation of x and y ordinates,

$$x = \exp^{random(x)t} \tag{10}$$

$$y = \exp^{random(y)t} \tag{11}$$

Where "random( )": is a function which generates random numbers t for a given time period.

An example is given in the Figure 2 below.

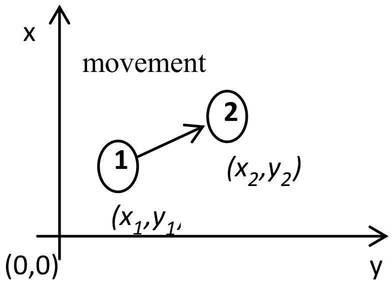

Figure 2: Movement of a node

The motion factor (M_f) is calculated using the direction of movement of the node and the speed of the node, to a given time period(t).

$$M_f = \frac{dy}{dt}\,((e^{\Delta xt} + e^{\Delta yt})) \tag{12}$$

3.2 Trust Calculation

As mentioned before the trust calculation is performed by considering the node behavior. In order to define this unique behavior of a node the above mentioned parameters are taken into consideration.

$$T_k = \frac{\sum (PDR_{aodv_k} + PDR_{cbr\_data_k}) + P_{r_{(k,m)}}}{M_{f_{(k,m)}}} \tag{13}$$

Where,

T_k	: Trust value for node k
k	: neighbor node k
m	: node m
PDR_{aodv_k}	: AODV control packet delivery ratio for node k
$PDR_{cbr\_data_k}$	: Data packet delivery ratio for node k
$P_{r_{(k,m)}}$	: Link positioning between node k and node m
$M_{f_{(k,m)}}$	: Velocity of node k with respect to node m

3.2.1 Trust Weightages

Following Table 2 shows the numerical values associated with the trust levels in the proposed model.

Table 2. Trust Degree Table

Value	Mean	Description
T_k<1	Untrusted	Malicious node
T_k≥1	Trusted	100% trusted

3.3 Modified Trust based AODV Routing Algorithm

The basic route learning algorithm in AODV routing protocol is changed as shown in Figure 3 below.

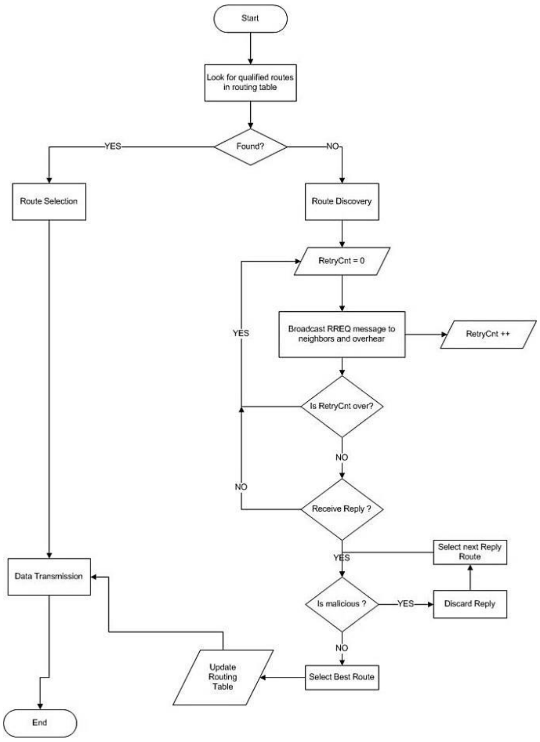

Figure 3: Trusted Routing Algorithm

4. SIMULATION, RESULTS AND ANALYSIS

Simulation has been conducted using NS-2 version 2.35. A route discovery evaluation process was carried out including malicious nodes to in both aspects of the normal AODV and the newly modified Trusted AODV. For all these measurements AWK scripts are used.

4.1 Performance Matric

- Packet Delivery Ratio (PDR) the ratio of the number of delivered data packet to the destination. PDR reflects the network processing ability and data transferring ability, and as the main symbols of reliability, integrity, effectiveness and correctness of the protocol.

- End to end delay in mille seconds is the total delay taken to transmit and receive all the data packets within a scenario.

- Throughput in kilobits per second is the throughput is measured as a ratio between the actual number of packets sent by the source node and the total time taken to transfer these packets. The transfer time is a sum of the actual time taken to transmit the packets and the overhead time incurred in implementing message request and flow control mechanisms. Data packets dropped en route to the destination are not taken into consideration for this metric.

4.2 Parameters and Topology

The simulation was carried out in a fixed number of node environments 50 mobile nodes, moving in an area of 1500 meters x 1500 meters square for 50 seconds simulation time. I use random waypoint mobility model, and transmission range is 250 meters. In the simulation, the speed are varied from 10 m/s to 50 m/s. The data traffic is Constant Bit Rate (CBR). The node starts in a single location and starts moving randomly in different velocities. Node 4 will communicate to node 49. Some nodes are by force made as malicious nodes such as node 25, 42, 45 and 19. So according to the environment node 4 is initiating a route discovery to node 49 in the presence of some malicious nodes. The Table 4 shows the simulation parameters for 50 nodes.

Table 4. Simulation Parameters for route discovery evaluation

Parameter	Value
Simulation time	50s
Topology	1500 m x 1500 m
Number of Nodes	50
Speed	Randomly varying from 10 m/s
Pause time	20 s
Traffic type	CBR
Mobility model	Random way point
Packet size	1000 bytes
Malicious nodes	1-10

The nodes maintain and update its neighbors trust values depending upon the behavioral aspects of them. The trust values further refine as the trust model matures with passage of time. During route discovery, the computed trust levels are associated as weights to the locally maintained routing tables. Any sending node can then verify if a certain route provides the adequate level of trust required for communication with a particular destination. Figure 4 demonstrates the application of the trust model to route discovery. Assuming that node 4 is initiating route discovery to node 40 in the presence of malicious nodes (25, 13, 29, 42, and 46). Malicious nodes carry out attack scenarios of DOS attacks and blackhole attacks.

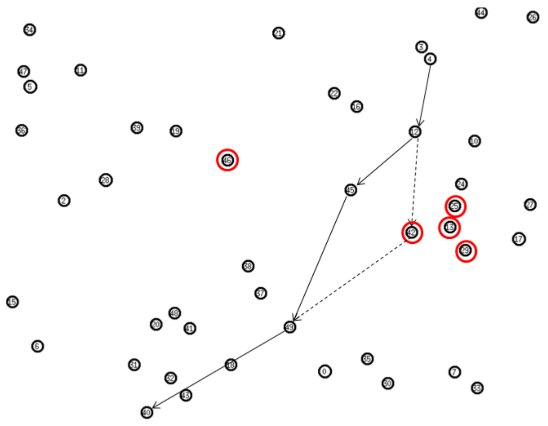

Figure 4: Trusted Route Discovery evaluation topology

4.3 Simulation Results

The simulations were carried out for the modified trusted AODV and normal AODV evaluating three factors. The Table 5 and 6 given below indicates the results.

Table 5. Simulation results for PDR, Delay and in Performance Evaluation

No. of Nodes	PDR		End to end delay (ms)	
	Normal AODV	Trust AODV	Normal AODV	Trust AODV
1	99.9	99.9	54.3	65.8
2	99.9	99.9	65.4	66.5
3	99.8	99.9	67.1	70.1
4	99.5	99.9	68.7	64.2
5	99.4	99.9	68.7	68.7
6	99.1	99.9	69.1	66.7
7	98.9	99.9	69.3	65.4
8	98.8	99.9	69.9	67.1
9	98.8	99.9	69.9	65.8
10	98.8	99.9	70.1	66.1

Table 6. Simulation results for PDR, Delay and in Performance Evaluation

No. of Nodes	Throughput(kbps)	
	Normal AODV	Trust AODV
1	111.7	136.5
2	136.5	136.5
3	136.5	136.5
4	136.3	136.5
5	136.3	136.5
6	136.2	136.5
7	135.0	136.5
8	134.6	136.5
9	134.5	136.5
10	134.2	136.5

4.4 Result Analysis

Figure 5 shows the result of packet delivery ratio under attack scenario with varies speed.

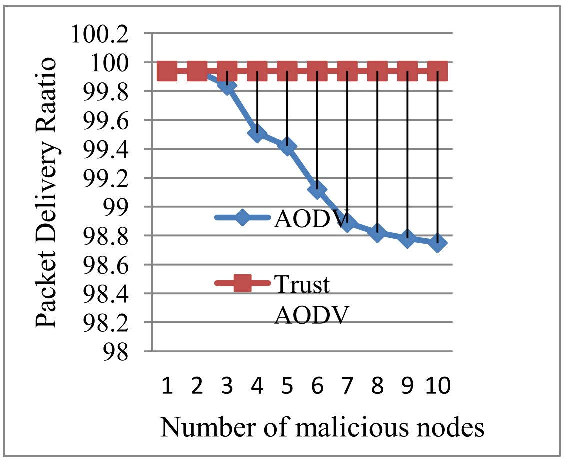

Figure 5: Packet delivery ratio vs number of malicious nodes

The proposed protocol can find the attacker node or the malicious node directly and ignores the malicious node. In comparison with the basic AODV which reflects the incapability of identifying such malicious node environments, it can be seen that the modified trusted AODV shows significant performance over varying number of malicious nodes. The packet delivery relation value of the proposed protocol is stable between 95% until 100%. This means the proposed mechanism can guarantee the packet delivery to the destination.

The trusted AODV protocol directly isolates the attacker and it will stop the attacker to send fake reply to the victim. Due to the attacker node cannot participate in the network; communication is running as there is no attack in the network. According to Figure 5, packet delivery ratio of the proposed protocol shows more stability as the number of attacker nodes or malicious nodes increases, than the other.

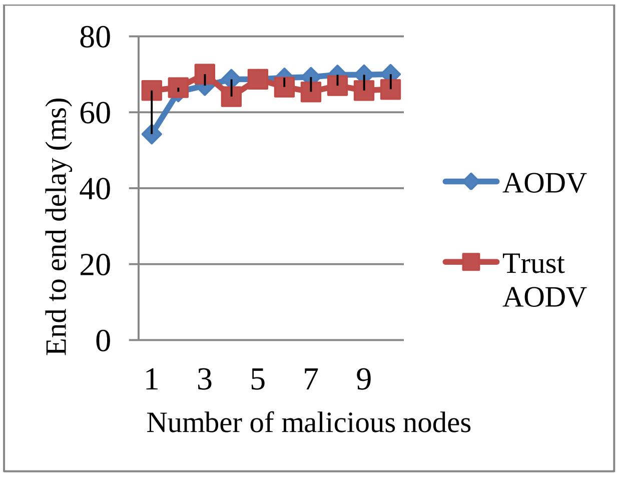

Figure 6: End to end delay vs number of malicious nodes.

It can be seen from Figure 6 when the end to end delay between the trusted and basic AODV protocols results in average constant values with very few fluctuations. Since the Trusted AODV includes the capability of identifying and isolating a malicious node from the communication path, there is a slight decrease in the delay factor, when compared with the basic AODV.

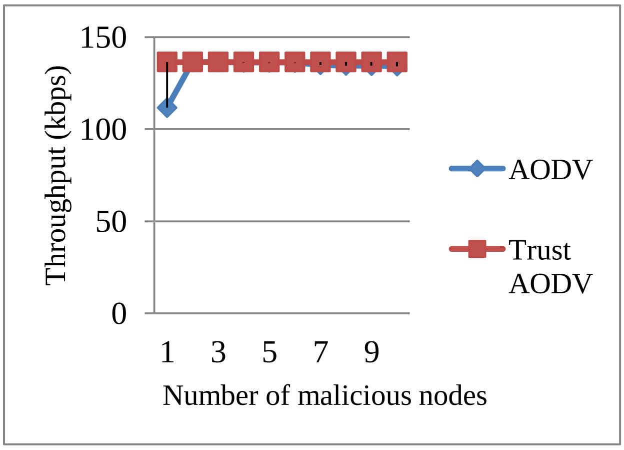

Figure 7: Throughput vs number of malicious nodes

In general, it can be seen that the throughput of both the normal AODV and trusted AODV shows the same near throughput values. This is mainly because that the resultant of the packet delivery ratio and the end to end delay component resultants. It can be seen that the resultant of the both will be very similar values that a slight variation with each other.

Over all, the performance of the trusted AODV protocol outperforms the existing basic AODV routing protocol with packet delivery ratio and end to end delay. Due to early detection and directly ignore the malicious node. The trust mechanism is performed even in an absence of a malicious node for proper validation. In addition the proposed mechanism does not add any new control messages to the existing AODV protocol, hence no additional computational is needed nor high overhead on the network. It incorporates a simple mechanism to provide authentication based security without encryption, thus less complex.

Some advantages include;

- Since each node has own trust calculation level to its neighbor, no need to perform warning mechanism to whole network.
- No extra memory is needed to store the status of the nodes science the trust calculation is performed each time the node starts communication.

5. CONCLUSION

The authors have reviewed some of secure routing protocols based on AODV and explored the security problems in wireless Ad hoc networks. The authors have also explored the variant of secure routing protocol based on AODV. Hence there are basically two mainstreams available to incorporate the security aspects in to AODV routing protocol i.e. cryptographic mechanism and trust based mechanism.

The authors address the security aspects and proposed a new trust mechanism that includes the capability on detecting and preventing the attack potentials into a wireless Ad hoc network especially for DOS and blackhole attack. Especially the proposed trust calculation is enhanced by adhering three behavioral factors of a node with respect another node.

The simulation analysis results indicate that the performance of the proposed trusted AODV protocol shows significance improvements over the existing basic AODV protocol, in terms of packet delivery ratio and end to end delay specially under larger number of attacker or malicious nodes.

6. FUTURE WORK

The proposed trust mechanism can be further extended to incorporate different levels of trust weightage levels to provide more options on communication environment for unpredictable Ad hoc network situations.

Also the mechanism can be further extended so that it includes the capability to detect another type of attack and apply a bio inspired algorithm to select the shortest and secure path.

Finally the most important approach is to trying to apply this method for a real network.

7. ACKNOWLEDGMENT

This research project was conducted as a compulsory component in completion for the degree of Master of Science in Information Technology at Sri Lanka Institute of Information Technology.

8. REFERENCES

[1] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks.”, Wireless Network Security, Signals and Communication Technology 2007, pp 103-135

[2] Kaushik,N., Dureja, A., “A Comparative Study Of Black Hole Attack In Manet.”, International Journal of electronics and communication Engineering & Technology, Volume4, Issue 2, March-April, 2013, pp. 93-102

[3] S. Corson, J. Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. IETF RFC2501, 1999.

[4] HongMei Deng, Wei Li, Dharma P. Agrawal. Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine, October 2002, p70-75.

[5] Abusalah, L., Khokhar, A., Guizani, M.: A Survey of Secure Mobile Ad Hoc Routing Protocols. IEEE Communications Surveys & Tutorials 10(4), 78–93 (2008)

[6] Johnson, D.B., Maltz, D.A.: Dynamic Source Routing in Ad hoc Wireless Networks. In: Mobile Computing, pp. 153–181. Kluwer Academic Publishers (1996)

[7] Zapata, M.G.: Secure adhoc on-demand distance vector (S-AODV) Routing. In: Proceeding of ACM Workshop on Wireless Security (WISE), Atlanta (2002)

[8] Yi, S., Naldurg, P., Kravets, R.: A Security-Aware Routing Protocol for Wireless AdHoc Networks. In: ACM Symposium on Mobile Ad Hoc Networking & Computing (ACM Mobihoc 2001), Short paper, Long Beach, CA, USA (October 2001)

[9] M Abolhasan, B Hagelstein & JC-P Wang, Real-world performance of current proactive multi-hop mesh protocols, IEEE APCC, Shanghai, China, 8-10th October 2009

[10] Perkins, Charles E. and Bhagwat, Pravin. “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”,1994.

[11] Akhlaq, M., Noman Jafri, M., Khan, M.A., Aslam, B.: Addressing Security Concerns of Data Exchange in AODV. Transactions on Engineering, Computing and Technology 16, 29–33 (2006) ISSN 1305-5313

[12] Cerri, D., Ghioni, A.: Securing AODV: The A-SAODV Secure Routing Prototype. IEEE Communications Magazine 46(2), 120–125 (2008)

[13] Eichler, S., Roman, C.: Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC. In: 2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 481–484 (October 2006)

[14] Pirzada, A.A., Datta, A., McDonald, C.S.: Trustworthy Routing with the AODV Protocol. In: The International Networking and Communications Conference (INCC 2004), pp. 19–24. IEEE Communications Society, Lahore (2004)

[15] Menaka, A., Pushpa, M.E.: Trust Based Secure Routing in AODV Routing Protocol. In: IMSAA 2009 Proceedings of the 3rd IEEE International Conference on InternetMultimedia Services Architecture and Applications. IEEE Press, Piscataway (2009)

[16] Zhe, L., Jun, L., Dan, L., Ye, L.: A Security Enhanced AODV Routing Protocol. In: Jia,,X., Wu, J., He, Y. (eds.) MSN 2005. LNCS, vol. 3794, pp. 298–307. Springer, Heidelberg (2005).

[17] Kurosawa, S., Nakayama, H., Kato, N., Nemoto, Y., Jamalipour, A.: Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method. International. Journal of Network, Security 5(3), 338–346 (2007).