International Journal of Management, IT & Engineering
(ISSN: 2249-0558)

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1	**Quality Improvement through SPC Techniques: A Case Study.** Dr. D. R. Prajapati	1-35
2	**Maximization of Return on Investment (ROI) by Hyper Productive Software Development Through Scrum.** Muhammad Inam Shahzad, Tasleem Mustafa, Fahad Jan, Muhammad Ashraf and Ahmad Adnan	36-60
3	**The design of a Trusted Authentication scheme for Wimax Network.** Mr. Rajesh Shrivastava and Deepak Kumar Mehto	61-80
4	**Highly Quantitative Mining Association Rules with Clustering.** N. Venkatesan	81-98
5	**An Efficient Routing Scheme for ICMN.** K. Soujanya, R. Samba Siva Nayak and M. Rajarajeswari	99-116
6	**Controlling the Menace of Unsolicited Electronic Mails – Contemporary Developments and Indian Perspectives.** Sachin Arora and Dr. Dipa Dube	117-151
7	**Comparing Search Algorithms of Unstructured P2P Networks.** Prashant K. Shukla, Piyush K. Shukla and Prof. Sanjay Silakari	152-165
8	**Determination of Lot Size in the Construction of Six sigma based Link Sampling Plans.** R. Radhakrishnan and P. Vasanthamani	166-178
9	**Construction of Mixed Sampling Plans Indexed Through Six Sigma Quality Levels with Chain Sampling Plan-(0, 1) as Attribute Plan.** R. Radhakrishnan and J. Glorypersial	179-199
10	**Analysis of optical soliton propagation in birefringent fibers.** Ch. Spandana, D. ajay kumar and M. Srinivasa Rao	200-213
11	**Design of Smart Hybrid Fuzzy Pid Controller for Different Order Process Control.** Anil Kamboj and Sonal Gupta	214-228
12	**Privacy and Trust Management in Cloud Computing.** Mahesh A. Sale and Pramila M. Chawan	229-247
13	**Sec.AODV for MANETs using MD5 with Cryptography.** Mr. Suketu D. Nayak and Mr. Ravindra K. Gupta	248-271
14	**Implementation of Image Steganography Using Least Significant Bit Insertion Technique.** Er. Prajaya Talwar	272-288

Editorial Board

Mr. SANJAY ASATI
Dept of ME, M. Patel Institute of Engg. & Tech., GONDIA(M.S.)

Mr. G. Y. KUDALE
N.M.D. College of Management and Research, GONDIA(M.S.)

Editorial Advisory Board

Title

SEC.AODV FOR MANETS USING MD5 WITH CRYPTOGRAPHY

Author(s)

Mr. Suketu D. Nayak
4th Sem M.Tech Computer Science & Engineering
Rajiv Gandhi Prodhyogiki Vishwavidhyalaya
Bhopal, India

Mr. Ravindra K. Gupta
Asst. Professor, CSE Dept.,
SSSIST, Sehore,
MP, India

Abstract:

Mobile Ad hoc Networks (MANETs) characteristics present major vulnerabilities in security. The threats which thought-out in MANETs are due to maliciousness that intentionally disrupts the network by using variety of attacks and due to insecure routing protocols (e.g. AODV), which were developed without considering security in mind. Due to lack of the infrastructure, open peer-to-peer architecture, shared wireless medium, limited resource constraints and highly dynamic topology, MANETs (Mobile Ad-hoc Networks) are frequently established in insecure environments, which make them more vulnerable to attacks. These attacks are initiated by sharing malicious nodes against different services of network. Ad-hoc On-Demand Distance Vector (AODV) is one such widely used routing protocol that is at present undergo extensive research and development. AODV is based on distance vector routing, but here the updates are shared not on a periodic basis but on an as per demand basis. The control packets contain a hop-count and sequence number field which recognizes the freshness of routing. These fields are editable, so it creates a possible susceptibility that is frequently abused by malicious nodes to advertise false better routes. As well as, transmission of routing updates in form of clear text also reveals crucial information about the network topology, which is again a probable security danger. In this paper we are presenting a novel and practical security mechanism for securing the AODV routing protocol that protects against a number of attacks carried out in MANETs. We will present message digest with secret key mechanism to secure AODV messages which is very effective and less power consuming security solution for MANETs.

Keywords - Malicious, Mechanism, Message Digest, Routing Protocol, Secret Key, Security

INTRODUCTION:

MANET is a collection of independent mobile users that communicate over relatively bandwidth and power constrained wireless links [1]. MANET has capability to establish networks at anytime, anywhere. These networks are built, work and maintained by its own because each node performs dual role of host and router. By and large, these nodes have a limited transmission range and so each node search for the support of its neighboring nodes in forwarding packets. In order to establish routes between two nodes which are away from each other than a single hop,

special routing protocols are already designed. This unique feature is responsible to route the message in spite of dynamic topology of network [2]. These networks don't depend on extraneous hardware which makes them an ideal candidate for military services and operations. For example battle field ad hoc network, in such a network we would surely be first concerned with the efficient and in time delivery of the message but with this, we will have to be more concerned about the strong privacy or secrecy of the information also. These kinds of scenarios, where we want to transmit private and secure information very rapidly, motivate us to make use of message digest with secret key in security context. In this paper we consider advantage of message digest with secret key to hide the information of all the fields of message by using different message digest functions.

PREVIOUS WORK:

To protect MANET against various possible attacks a routing protocol must fulfill a set of requirements [3] to confirm that the determined path from source to destination works correctly in the presence of malicious nodes. These requirements are:

1) Authorized nodes should perform route computation and discovery,
2) Minimal exposure of network topology,
3) Detection of spoofed routing messages,
4) Detection of fabricated routing messages,
5) Detection of altered routing messages,
6) Avoiding formation of routing loops, and
7) Present redirection of routes from shortest paths.

Many secure routing protocols have been recently developed that conform to most of the requirements. Some of them are as under:

1. SAODV (Secure Ad-hoc On-Demand Distance Vector)

SAODV [8] is an extension of AODV routing protocol. It provides authentication, message integrity and non-repudiation in ad-hoc networks by using one-way hash chain and digital

signature. It needs the use of Key Management Scheme. The main disadvantage with the protocol is the use of Public Key Cryptography that requires considerable amount of processing power and slows down the process to some extent.

2. ARAN (Authenticated Routing for Ad-hoc Networks)

ARAN [3] provides authentication, message integrity and non-repudiation in ad-hoc networks by using a preliminary certification process which is followed by a route instantiation process that ensures end-to-end security services. But it needs the use of trusted certification server. The main disadvantage with the protocol is every node that forwards a route discovery or a route reply message must also sign it, which is very power consuming and causes the size of the routing messages to increase at each hop.

AODV ROUTING PROTOCOL:

AODV [2] is a distance vector routing protocol that has been naturally build for MANETs. It is an on demand protocol and reactive in nature as it searching the routes only when required. It makes use of basic route establishment and maintenance mechanisms from the DSR protocol and hop-to-hop routing vectors from the DSDV protocol. AODV makes widespread use of sequence numbers in control packets to avoid the problem of generation of routing loops. When a source node is interested to communicate with a destination node whose route is unknown, it broadcasts a RREQ (Route Request) packet. Each RREQ packet contains a Request ID, source and the destination node IP addresses and sequence numbers along with a hop count and flags. The Request ID field uniquely identifies the RREQ packet; the sequence numbers gives information regarding the freshness of control packets and the hop-count maintains the number of nodes between the source and the destination. Recipient node of the RREQ packet that has not find the Source IP and ID pair or doesn't maintain a fresher (larger sequence number) route to the destination rebroadcasts the same packet after incrementing the hop-count. Such intermediate nodes also create and preserve a REVERSE ROUTE to the source node for a certain time.

When the RREQ packet arrived at the destination node or any intermediate node that has a fresher route to the destination a RREP (Route Reply) packet is generated and sent back to the source. RREP packet contains the destination node sequence number, the source and the

destination IP addresses, route lifetime along with a hop count and flags. Intermediate node that receives the RREP packet, increments the hop count, establishes a Forward Route to the source of the packet and transmits the packet on the Reverse Route. AODV makes use of HELLO messages periodically to find link failures to nodes that it considers as its immediate neighbors. When a link failure is detected for a next hop of an active route a RERR (Route Error) message is sent to its active neighbors that were using that particular route.

The key vulnerabilities [2] present in the basic AODV routing protocol are:

1) Deceptive incrementing of Sequence Numbers
2) Deceptive decrementing of Hop Count

Value	Hash Function
0	Reserved
1	MD5
2	SHA1
3-127	Reserved
128-255	Implementation Dependent

Table 1: Possible values for Hash_Function field

SECURING AODV USING MESSAGE DIGEST AND SECRET KEY MECHANISM:

There is a Message Digest with Secret Key mechanism used to secure AODV message. This mechanism calculates message digest using appropriate hash function for all the fields (mutable as well as non-mutable) of an AODV message in addition with secret key. And then message digest and hash function value will be transmitted along with the AODV message.

The Message Digest with Secret Key mechanism algorithm is as follows:

- Every time a node originates a RREQ, a RREP or a RERR message, it performs the following operations:
  - It chooses suitable value of hash function h that is to be used to make message digest, from all available possible values shown in Table 1.
  - Sets Hash_Function field by value of chosen h.

    Hash_Function = h

    Where, h is the value of hash function.
  - Get the value of Secret Key, and add it to values of all the fields of message.
  - Calculates Message_Digest by passing the values of all the fields with added secret key to hash function h.

    Message_Digest = h (values of all the fields with added secret key)

    Where, h is a hash function.

    h(x) is the result of applying the function h to x.
- In addition, every time a node receives a RREQ, a RREP or a RERR message, it performs the following operations in order to verify the valid message:
  - Get the value of Secret Key, and add it to values of all the fields of received message.
  - Applies the hash function h to the values of all the fields of received an AODV message with added secure key except Hash_Function and Message_Digest fields, and verifies that the calculated message digest is equal to the value contained in the Message_Digest field of received an AODV message.

    Message_Digest = = h (values of all the fields with added secure key except Hash_Function and Message_Digest fields)

    Where, a = = b reads: to verify that a and b are equal.
  - Before rebroadcasting a RREQ or forwarding a RREP or a RERR, a node will perform the following:

- It once again chooses suitable value of hash function h (may be different of earlier value of h) that is to be used to make message digest.
- Sets Hash_Function field by value of chosen h.

  Hash_Function = h
- Get the value of Secret Key, and add it to values of all the fields of message.
- Calculates Message_Digest by passing the values of all the fields to hash function h.

  Message_Digest = h (values of all the fields with added secret key)

EXTEDED MESSAGE FORMATS:

Type	J	R	G	Reserved	Hop Count
RREQ ID					
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Originator Sequence Number					
Hash Function	Message Digest				

Figure 1: Secure AODV RREQ Message Format

Type	R	A	Reserved	Prefix sz	Hop Count
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Lifetime					
Hash Function	Message Digest				

Figure 2: Secure AODV RREP Message Format

Type	N	Reserved	Dest Count
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable Destination IP Address (if needed)			
Additional Unreachable Dest. Sequence Number (if needed)			
Hash Function	Message Digest		

Figure 3: Secure AODV RERR Message Format

As shown in Fig. 1, Fig. 2 and Fig. 3, the extended fields namely Hash Function and Message Digest (shown in gray color) are added in AODV messages [13], in order to make them secure according to our proposed mechanism.

MESSAGE DIGEST WITH SECRET KEY MECHANISM:

In our proposed secure mechanism, we assumed that there exists a central key management system, which distributes secret key to all legitimate nodes in advance before they participate in system called a team key or a group key or anything else. How key management system handles, distribute and share the secret key among legitimate nodes is out of scope for this paper.

The detail secure Message digest with secret key mechanism works as shown in Figure 4.

The node which wants to send AODV message, first selects appropriate hash function and then gets secret key and adds secret key to the message data and then applies hash function on message data with added secret key to create message digest, after creating message digest it will send message digest and hash function value along with AODV message to the next node. The node which receives AODV message first obtains hash function from received hash function value and then gets secret key and

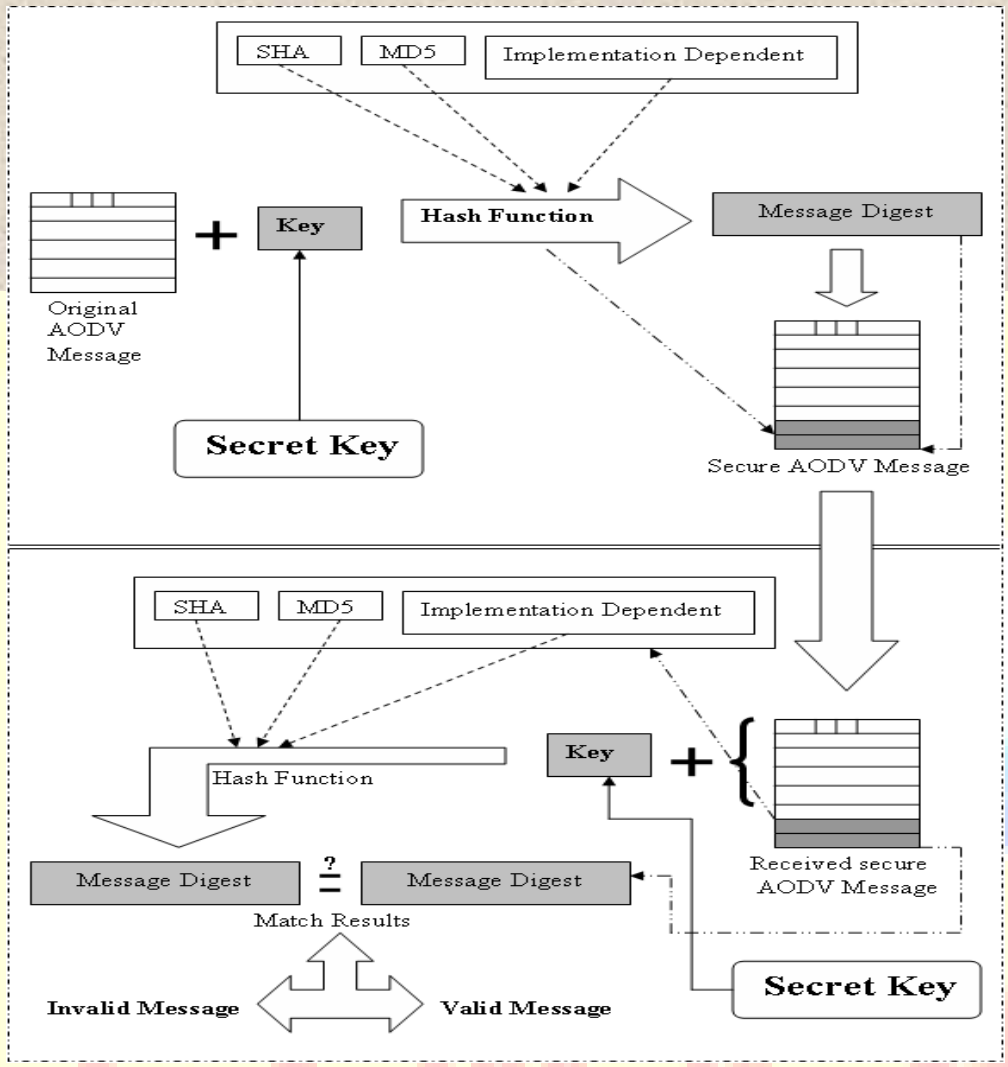

Figure 4: Message digest with secret key mechanism

adds secret key to the message data of received message and then applies that hash function on message data of received message with added secret key and creates message digest. After creating message digest it will compare created message digest with received message digest, if both message digests are equal it will accept that valid message and process it, but if they are not equal it will not accepting that invalid message and simply drops it.

SIMULATION AND RESULTS

We have successfully implemented message digest mechanism to secure AODV routing protocol using NS-2.34 on UBuntu Linux version and concluded that it is very secure mechanism which fulfills all security requirements without consuming much power of nodes and gives almost same performance as AODV gives without using mechanism.

Parameter	Value
MANET Area	500*500 sq. m.
Total number of nodes	25
Movement Pattern	Non-random
Node Speed	0 up to 20 m/s
Application	Constant Bit Rate (CBR)
Number of generated Packets	10000 packets per CBR
Size of Packet	512 bytes
Simulation Time	100 sec

Figure: 5 Simulation Parameter

The simulation experiments are developed and simulated on an Intel Core2Duo 1.83 GHz machine using Ubuntu 9.10 with 2 GB RAM and the network simulator NS2 version NS-2.34.

The below table summarized the different configuration values that were used in all the performed simulations.

Routing Protocol: Simple AODV **Case:** With or without malicious node 47						
Node	**Packets**					
	Generated	**Sent**	**Forwarded**	**Dropped**	**Lost**	**Received**
All	16322	14882	2721	1578	265	--
Node 47	254	2	119	20	0	4283

The below table summarized the different configuration values that were used in all the performed simulations.

Routing Protocol: AODV with proposed security mechanism **Case:** Without malicious node						
Node	**Packets**					
	Generated	**Sent**	**Forwarded**	**Dropped**	**Lost**	**Received**
All	16322	14882	2721	1578	265	--
Node 47	254	2	119	20	0	4283

Routing Protocol: AODV with proposed security mechanism **Case:** With malicious node 47						
Node	**Packets**					
	Generated	**Sent**	**Forwarded**	**Dropped**	**Lost**	**Received**
All	16391	15014	2845	1518	324	--
Node 47	257	0	0	14	0	4052

Simulation Environment for 60-Node Scenario

For simulation, there are 60 different mobile nodes considered, namely node 0 to node 59 in a space of 1500*300 square-meters. Total simulation time is 400 sec. All network components of mobile node are considered their default values, e.g. Link Layer, Interface Queue, Mac layer etc. CBR traffic is “mobility/scene/cbr-50-20-4-512” and Movement scenario is “mobility/scene/scen-1500X300-60-0-20-2” from ns-allinone-2.34 package.

Simulation Results for 60-Node Scenario

Table 2: AODV with or without malicious node 47

Table 3: AODV with proposed security mechanism and without malicious node

Routing Protocol: SAODV **Case:** With malicious node 47						
Node	**Packets**					
	Generated	**Sent**	**Forwarded**	**Dropped**	**Lost**	**Received**
All	16754	15357	2511	1520	436	--
Node 47	264	0	0	18	0	4292

Table 4: AODV with proposed security mechanism and with malicious node 47

Routing Protocol: SAODV **Case:** Without malicious node						
Node	Packets					
	Generated	Sent	Forwarded	Dropped	Lost	Received
All	18524	17081	2557	1584	689	--
Node 47	287	5	44	28	0	4716

Table 5: SAODV without malicious node

Table 6: SAODV with malicious node 47

We have successfully implemented message digest mechanisms to secure AODV routing protocol in NS-2.34 network simulator on UBuntu Linux version and concluded that it is very secure mechanisms which fulfills all security requirements without consuming much power of nodes and gives almost same performance as AODV gives without using security mechanism.

Table 2 shows that simple AODV routing protocol cannot detect any malicious node/s and generate, send, forward, dropped, lost and receive same amount of packets in both the cases of present and absent of malicious node/s.

Table 3 shows that AODV routing protocol with proposed mechanism and without any malicious nodes in system will generate, send, forward, dropped, lost and receive same amount of packets as AODV will generate, send, forward, dropped, lost and receive.

Table 4 shows AODV routing protocol with proposed mechanism and with malicious node 47 that can easily detect malicious node. Here network recognizes that node 47 is malicious and will not forward any of the messages to node 47. So that both of the values of sent and forwarded packets are 0.

Table 5 shows that SAODV routing protocol without any malicious nodes in system will generate, send, forward, dropped, lost and receive different amount of packets as AODV will generate, send, forward, dropped, lost and receive.

Table 6 shows SAODV routing protocol with malicious node 47 that can easily detect malicious node. Here network recognizes that node 47 is malicious and will not forward any of the messages to node 47. So that both of the values of sent and forwarded packets are 0.

Above discussion and results easily illustrates that proposed mechanism is very efficient, secure and can easily finds malicious node within system, provides good security overall.

Simulation Results:

In this, the results of the various performed simulations are presented. The main focus of the simulations is two scenarios. The first scenario is to simulate routing performed using SAODV, in other words, to simulate secure AODV secure routing protocol. The second scenario is to simulate the routing performed with the proposed message-digest security scheme, in other words, to simulate the newly proposed security mechanism. In the following sections, the results of the simulation runs comparing between SAODV and the proposed –AODV with message digest mechanism and using different simulation metrics are presented

No. of Packets Calculated:

In order to measure packet delivery fraction and routing load, it is necessary to calculate total number of sent, received and routed packets. Following table shows total number of sent, received and routed packets for given simulation environment. All Packets are calculated using shell script.

Protocol	Pause Time	CBR Traffic					
		10			20		
		S	R	RT	S	R	RT
AODV/ AODV-MD/ AODV-MDS	0	4452	4427	630	6777	5867	1884
	10	4505	4489	587	6796	6659	1630
	20	4421	4392	544	6830	6592	1084
	40	4472	4456	420	6801	6547	914
SAODV	0	4437	4426	521	6803	6248	1167
	10	4505	4489	587	6778	6306	1815
	20	4433	4415	552	6789	6425	847
	40	4439	4428	448	6794	6483	1050
	100	4455	4453	223	6793	6790	376

S – Sent Packets R- Received Packets RT- Routed Packets

Table 7: Number of sent, received and routed packets for different CBR traffic and at different pause time

Moreover, the same values shown in table are also given in graphical format to compare number of packets for different criteria for both protocols.

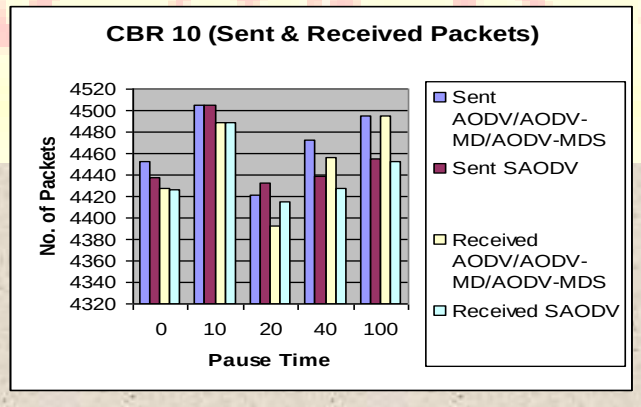

Fig 6: Sent & Received Packets for CBR traffic 10

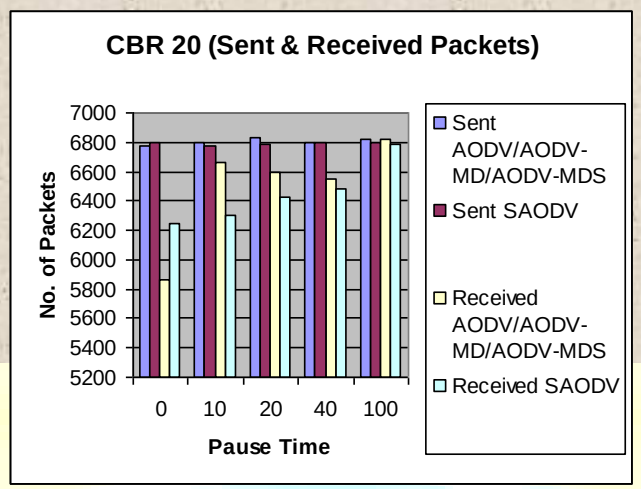

Fig 7: Sent & Received Packets for CBR traffic 20

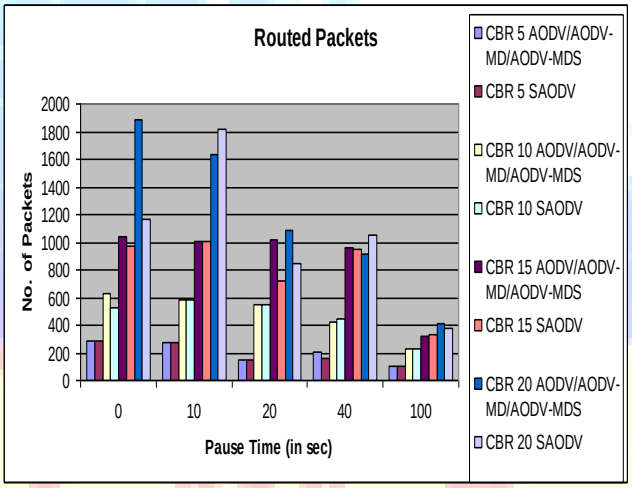

Fig 8: Router Packets for different CBR traffic at various pause time

Experiment:

Packet Delivery Fraction: In this experiment, the packet delivery fraction is being measured for the SAODV secure routing protocol and the proposed-AODV with message digest mechanism. The pause time and the CBR traffic of nodes participating in the mobile ad hoc network are varied to compare the results.

Results:

The below table shows the results of the packet delivery fraction of both protocols: SAODV and AODV with message digest mechanism with different pause time and CBR traffic. In given below figures, PDF value is in between 0 to 1 and pause time is in seconds.

Protocol	Pause Time	CBR Traffic	
		10	20
AODV/ AODV-MD/ AODV-MDS	0	0.994384546	0.865722296
	10	0.996448391	0.979841083
	20	0.993440398	0.965153734
	40	0.996422182	0.962652551
	100	1.000000000	0.999413748
SAODV	0	0.997520847	0.918418345
	10	0.996448391	0.930362939
	20	0.995939544	0.946383856
	40	0.997521964	0.954224316
	100	0.999551066	0.999558369

Table 8: PDF values for both protocols at different pause time and for different CBR traffic

Experiment:

Routing Load: In this experiment, the routing load is being measured for the SAODV secure routing protocol and the proposed-AODV with message digest mechanism. The pause time and the CBR traffic of nodes participating in the mobile ad hoc network are varied to compare the results.

Results:

The below table shows the results of the routing load of both protocols: SAODV and AODV with message digest mechanism with different pause time and CBR traffic. In given below figures, Routing Load (RL) value is in between 0 to 1 and pause time is in seconds.

Protocol	Pause Time	CBR Traffic	
		10	20
AODV/ AODV-MD/ AODV-MDS	0	0.142308561	0.321118118
	10	0.13076409	0.244781499
	20	0.123861566	0.164441748
	40	0.094254937	0.139605926
	100	0.050055617	0.060859364
SAODV	0	0.117713511	0.18677977
	10	0.13076409	0.287821123
	20	0.125028313	0.131828794
	40	0.101174345	0.161962055
	100	0.050078599	0.055375552

Table 9: RL values for both protocols at different pause time and for different CBR traffic

In this, the different results of the experimental work were presented. Throughout the different sections, the experiments' objective, result and analysis were stated. Also, this chapter ended up by showing that when CBR traffic is less, SAODV and AODV with proposed mechanism having almost same PDF values, but once when CBR traffic is increases AODV with proposed mechanism seems more efficient than SAODV. Further more, when CBR traffic is less, SAODV and AODV with proposed mechanism having almost same RL values, but once when CBR traffic is increases AODV with proposed mechanism seems more efficient in routing than SAODV.

CONCLUSION:

In this paper we have presented a message digest with secret key mechanism for securing the AODV routing protocol used in MANET. Research in the field of networks has shown that Public Key Cryptography and its related algorithms are very slower and power consuming than the Symmetric Key Cryptography. Our proposed mechanism uses symmetric key cryptography and generates very less overhead of calculations and saves power consumption of nodes significantly which is most important and attractive feature. This mechanism does not use any kind of encryption or decryption techniques so that the performance of secure routing protocol is remain almost same. The entire security strength of this mechanism is relies on how frequently key management scheme is changing the secret key of all nodes. For ensuring greater security, we can have the concept of "One Time Pads" or "Key of the Day" etc. Moreover, the military networks which perform very sensitive operations where we have to spread private information very securely, we are mainly concern about privacy or secrecy along with efficient and in time delivery of the message. Such a kind scenarios motivate us to use message digest with secret key which is very secure as well as efficient.

Last but not least, according to the many simulations that were performed, the newly proposed message digest-based scheme, built on top of normal AODV routing protocol, achieves a higher packet delivery fraction than SAODV. Thus, the proposed design, message digest based AODV, proves to be more efficient and less power consuming than SAODV secure routing protocol in defending against both malicious and unauthenticated nodes.

FUTURE WORK:

Some of the ideas that can be further integrated to the proposed message digest-based scheme are presented as follows:

- The same kind of message digest based mechanism can be designed to secure other routing protocols of MANET like DSR, DSDV, TORA etc.
- Message digest based mechanism using secret key can be enhanced by adding concept of "set of secret key", in which each node will maintain couple of secret keys instead of single unique key, in order to make presented mechanism more secure.

- The same kind of message digest based mechanism can be designed to secure sensor networks also.

REFERENCES:

- Junaid Arshad, Mohammad Ajmal Azad, "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks", (2006) IEEE, pp. 971-975.
- Asad Amir Pirzada, Chris McDonald, "Secure Routing with the AODV Protocol", (2005) Asia Pacific Conference on Communication, Perth, IEEE, p.p. 57-61.
- B. Dahill, B.N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks", Proceedings of the international conference on Network Protocols (ICNP), p.p. 78-87, 2002.
- Tuulia Kullberg, "Performance of the Ad hoc On demand Distance Vector Routing Protocol", HUT T-110.551 Seminar on Internetworking.
- Manel Zapata, N. Asokan, "Securing Ad hoc Routing Protocols" (2002), WiSe-02, September 28,2002, Atlanta, Georgia. (ACM)
- H Yang, H.Y. Lue, F Ye, S.W. Lu and L Zhang, "Securing in mobile as hoc networks: challenges and solutions" (2004) IEEE wireless communications 11(1), pp. 38-47.
- Jean-Pierre, Levente Buttyan, Srdan Capkun, "The Quest for security in mobile ad hoc networks". (2001) ACM.
- Manel Zapata, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, INTERNET DRAFT (September 2006) draft-guerrero-manetsaodv-06.txt
- Ns homepage - http://www.isi.edu/nsnam/ns/
- Ns manual - http://www.isi.edu/nsnam/ns/
- Konrad Wrona, "Distributed Security: Ad Hoc Networks & Beyond", PAMPAS Workshop, RHUL, September 16-17, 2002.
- Lin, Rad, Wong, Song, "Experimental Comparisons between SAODV and AODV Routing Protocols", WMuNeP, October 13, 2005. (ACM)
- Perkins, Belding-Royer and Das, "Ad hoc on-demand distance vector (aodv) routing", IETF RFC 3591, 2003.