DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4491

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A METRIC FOR MEASUREMENT AND SECURITY IN AD-HOC ROUTING PATHS

Esha Rani
Assistant Professor
University College, Kurukshetra,
India

Vikas Juneja
Assistant Professor
JMIT, Radaur Engg. College
Yamunanagar, India

Abstract: As in Manets, Dynamic topology is used; no infrastructure is there. The Ad-hoc on demand distance vector routing protocol (AODV) is outlined for mobile ad hoc networks (MANETs) to handle situations like dynamic link conditions; low memory overhead and low network utilization. But Security issues are not properly concerned; it remains a challenge for wireless designers. Various solutions have been proposed to establish a secure divulgation between end users by providing the security services like authentication, confidentiality, integrity, and availability, to mobile users; these solutions identify that the secure operation of AODV is a bi tier task (i.e. Routing and Secure interchange of information at separate levels). Most of the research work has been done in ad-hoc networks to resolve the problems such as routing coping with the new challenges caused by networks' and nodes' features without concerning the security issues into account. As security plays an increasingly important role in many systems, it is indispensable that we have a better understanding and management of computer security. We propose a framework to measure and enforce security attributes on ad hoc routing paths. The aim of this paper is to propose a Security Measurement (SM) framework includes "Computer Security"; a measure for computer security; a methodology to make best estimate of the measures; apply validation on measure.
The rest of this paper is organized as follows. In Section II we will give the brief description of MANETs and IEEE802.11. Section III will introduce about the different types of routing protocols. In Section IV an overview of Attacks against AODV is given. Section IV describes security principles. In section V security issues are discussed. Security Measurement Framework is introduced in section VI. At last, we conclude with recommendation plans for future work in Section VI.

Keywords: MANET; AODV; IEEE802.11; Security; Attacks; Routing

1. INTRODUCTION

i.) **MANETs:** Unlike traditional network, ad-hoc networks do not depend on any fixed infrastructure. User can access the data at any time from any location, makes the vision of wireless technology. User doesn't need to be bound with any device that makes the access more and more attractive. A mobile ad hoc network, or MANET, is a unstable network without infra-structure, formed by a set of mobile hosts (nodes or devices) [1]. Without the interference of central administration, all the nodes have right to dynamically establish their own network to communicate with each other by transferring the packets. This is a good but challenging task, since these devices or nodes have limited resources (Battery, space, CPU etc.). Problems are not over here Moreover; the network's environment has some features that add extra complications, such as the periodic topology variates caused by nodes' mobility, and the unreliability and the bandwidth limitation of wireless channels [1]. In earlier studies on the ad hoc networks, many solutions have been proposed to some fundamental problems, confronting the new challenges caused by networks' and nodes' features, these studies end to interesting new solutions. However, the problem with these results is that they do not take the security issues into account; hence, they are susceptible to threats. Whereas, many emanating applications designed for ad hoc networks necessitate robust security primitives and privacy protection. A robust security is also required to ensure fair and right functioning to the system, and to provide adequate quality of service in such an open vulnerable environment.

ii.) **IEEE802.11:** IEEE 802.11 is a widely used wireless network standard [2].Communication between users in the wireless network is possible by either connected the users in an infrastructure or ad hoc mode. Ad hoc wireless networks of mobile hosts (nodes) MANETs [3] are dynamic in nature. MANETs are characterized by bandwidth constrains, low physical security and power limitations. These networks comprise of a dexterous set of cooperating peers, which share their wireless capabilities with other congruent devices to enable communication with devices not in direct radio - range of each other [4]. Due to their multifaceted characteristics, ad hoc networks percolate on specific routing protocols.

2. ROUTING PROTOCOLS

Routing protocols in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner. The functional area of MANET protocol is effectively over a wide range of networking context from small ad-hoc group to larger mobile Multi-hop networks. There are two major classes of routing protocols associated with ad hoc

networks, proactive routing protocol and reactive routing protocol [5].

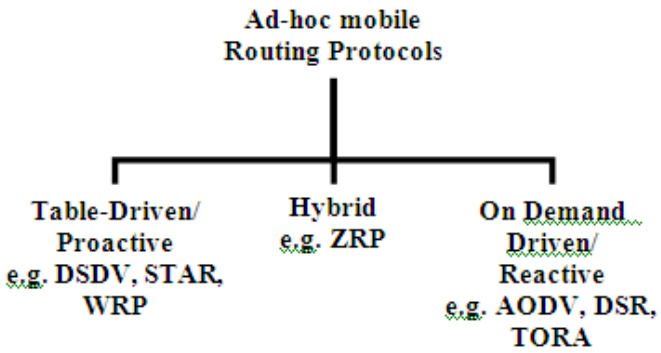

Fig.1 Hierarchy of Routing Protocols

Fig.1 shows the categorization of these routing protocols.

1. Proactive (Table Driven) protocol focus on maintaining consistent overview of the network, each node is constrained for broadcasting topology information at regular interval of time (e.g. DSDV) [6].
2. Reactive protocols are on demand protocols that discover the route once needed (e.g. AODV [7]). The reactive protocols exhibits extensive bandwidth and overhead advantages
3. Over proactive protocols. AODV routing protocol offers quick variation to dynamic link conditions, low processing, low memory overheads, and low network utilization [7]. AODV protocol is susceptible to security threats and any malignant intention may compromise its overall performance.

Governing security services, such as authentication, confidentiality, integrity and availability to mobile users is the extreme objective of the security solutions for AODV protocol. In order to achieve these goals, the security solution should maintain complete protection covering the entire protocol stack. Table I identifies the security issues in each layer [8]. In this article, we would contemplate in addressing security concerns related to data exchange. A modified protocol will be intended that assemble the routing, authentication, generation and secure exchange of session key in a single step. This would ease the users to enact parameters during the routing session and these parameters would subsequently be used to ensure confidentiality and integrity of data exchange.

Issues arises in security related to each layer [19] is discussed as follows:

1. Application Layer :: Malicious codes, Prevention, detection of viruses, worms, application abuses

2. Transport Layer :: Providing end to end data security through encryption techniques and Authentication

3. Network Layer :: Security of ad hoc routing protocols and associated parameters.

4. Physical layer :: Preventing signal jamming, denial of service attacks and other active attacks.

3. ATTACKS AGAINST AODV

It includes any action that intentionally aims to cause any damage to the network.

Types of Attacks:

Attacks can be viewed in two ways:

1. General view
2. Technical view

In General View, Attacks can be divided into three classes which are discussed as follows:

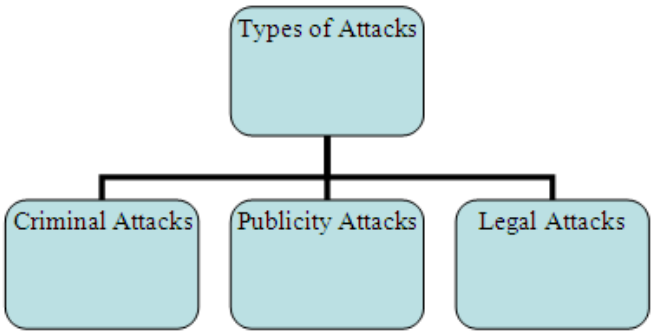

Fig.2 General view of attacks

1. **Criminal Attacks**: Aim of attackers is to maximize financial gain by attacking computer systems.
2. **Publicity Attacks:** In this attack, attackers want publicity of their names on newspaper and TV news channels and one form of this type of implementation is performed by damaging the web page of a Website. These attackers are usually not hand core criminals.
3. **Legal Attacks:** In this attack, attacker attacks the computer system and the attacked party manages to take the attacker to the court. While the case is being fought, the attacker tries to convince the judge and jury that there is inherent weakness in the computer system and she has done nothing wrong. The aim of the attacker is to exploit the weakness of the judge and the jury in technology matters.

In Technical View, Attacks can be divided according to origin and according to nature which are discussed as follows:

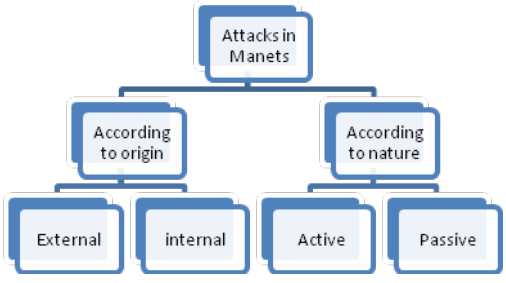

Fig.3 Technical View of Attacks

1. External attack

External attacks are introduced by outside of the network. It is caused by a node that does not belong to logical network. It causes congestion sends fake routing information or causes unavailability of services [9].

2. Internal attack

Internal attacks are introduced by a node that belongs to network. Unauthorized gain is accessed by malicious node and treated as an absolute node. Now it is accredited as a part of network and can participate in all activities of network. It can also estimate the traffic between nodes.

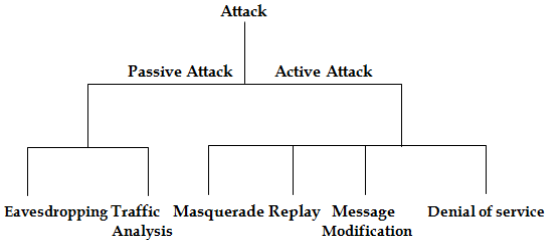

Fig.4 Examples of Active Passive Attack

3. Passive attack

The performance of the network is not actually disrupted by this attack. E.g. Snooping: Snooping is unauthorized access to another persons' data [10].

4. Active attack

An active attack pursuits to alter or destroy the data being exchanged in the network.

4. PRINCIPLES OF SECURITY

Security is the consolidation of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation [5], [11],[12]. In providing a secure networking environment some or all of the following services may be required:

A. Confidentiality

Only the sender and intended recipient should be able to access the contents of the message. Information readability should be restricted to only authorized members. Due to the open medium used by MANETs, usually all nodes within the direct transmission range can obtain the data. This is generally provided by encryption. Two types of encryption are commonly used.

1. Symmetric Encryption: In this encryption scheme, two nodes share a key (e.g. - DES, AES).Any data transmitted between the nodes is encrypted using this key. This key must be provided to the nodes over a secure channel. Symmetric encryption generally requires less computational resources than public key encryption. In *Public Key Encryption*, a public\private key pair *pubKn/privKn* is generated by all participating nodes. The node makes its public key *pubKn* available to all nodes. If other nodes wish to send data to node *n*, they encrypt their data using *pubKn*, safe In the knowledge that it can only be decrypted by *n*s' private key *privKn*, which only node n knows.[13]

B. Authentication

It requires a node to ensure the identity of the peer node it is communicating with. Both parties (Sender and Receiver) should be sure about the identities of each other. Without knowing the identity, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Encryption along with Cryptographic hash functions, digital signatures and certificates provide Authentication. Details of the construction and operation of digital signatures can be found in RFC2560. [13]

C. Integrity

It ensures to keep the message sent from being illegally altered or destroyed in the path. When the data in form of packet or message is sent through the wireless medium, the data can be modified or deleted by malicious attackers. The malicious attackers can also resend it, which is called a replay attack. The integrity service can be provided using cryptographic hash functions along with some form of encryption.

D. Non Repudiation

Non-repudiation does not allow the sender of a message to refute the claim of not sending that message. Non-repudiation requires the use of public key cryptography to provide digital signatures. A trusted third party is required to provide a digital signature.

5. ISSUES RELATED TO SECURITY

As environment of ad-hoc network is wireless or infrastructure less, nodes are more susceptible to attacks. That's why the key security issues must be taken care a lot to secure the network.

Peer-to-Peer Information Security: In the wireless environment the communication [14, 15, 16] between the nodes is more susceptible to attacks. No protection is provided in ad hoc network by firewall or access control. Any node can become vulnerable to attack from any direction. The identity of node could be imitated by the malicious node, it could disposition the node's identifications, it could leak the node's private information or it could pose as the node. This type of attack could leak the integrity, confidentiality and availability of the service provided by the node. The authentication and identification of node is also essential in ad hoc network. The main issue in the authentication and identification is that the nodes can be set to be authorized to gain access, without these methods the nodes may be given delegate certificates with which the node can access to the services. In some ad hoc networks the services may be centralized, while in other networks they are applied in distributed manner, which may require the use of different access control Mechanisms. Moreover the requisite security level in access control also affects the way the access control must be implemented. To ensure the peer-to-peer security, the traditional security mechanisms such as digital signature, authentication protocols and encryption are used in achieving the primary and secondary security goals for ad hoc network.

Secure Routing: The routing protocols [14,15,16] with in ad hoc networks are more susceptible to attacks as each device acts as a interface. Any tampering with the routing information can be compromise the whole network. An attacker can establish rogue information within routing information or replay old logged information.

The aim is to guard any information or behavior that can update or cause a change to the routing tables on cooperating nodes involved in an ad hoc routing protocol. To achieve completeness, ordering and timeliness are added to the list of enviable security properties that can remove or

lessen the threat of attacks against routing protocols. Techniques that can be used to promise these properties are described in Table II.

Table 1: Properties of Secure Routing

Properties	Techniques
Timeliness	Slotted Time
Ordering	Sequence Numbering
Authenticity	Password, Certificate
Authorization	Credential
Integrity	Digital Signature, Digest
Confidentiality	Encryption
Non-Repudiation	Chaining of Digital Signature

Reconciliation of routing protocol messages with these following properties is done to thwart attacks that exploit the susceptibility of damaged information in transit:

- **Timeliness:** On time delivery of messages show the true state of the links of routers on the network. Routing updates need to be delivered in a timely fashion. Update messages that arrive late, may reflect the challenging situation. It can cause incorrect forwarding or even circulate false information. Most ad hoc routing protocols have timestamps and timeout mechanisms to guarantee the sparkle of the routes they provide.
- **Ordering:** Out-of-order updates can also affect the accuracy of the routing protocols. These messages may not replicate the true state of the network and may circulate false information. Sequencing is used in ad hoc routing protocols that are distinctive within the routing domain to keep updates in order.
- **Authenticity:** Routing updates must create from authenticated nodes and users. Mutual authentication is the basis of a trust relationship. Easy passwords can be used for weak authentication. Each entity can add a public key certificate, attested by a trusted third party to claim its authenticity. A login mechanism in form of password is implemented by the certifying authority to authenticate the identity of the entities at the first place. The receiving node can then verify this claim by examining the certificate. One of the problems in ad hoc network is the absence of a centralized authority to issue and validate certificates of authenticity.
- **Authorization:** An authenticated user or node is issued an remarkable credential by the certificate authority. These credentials have the specification of permissions associated by the nodes. Currently, credentials are not used in routing protocol packets, and any packet can activate update propagations and modifications to the routing table.
- **Integrity:** In routing updates, the flow of information automatically can cause the routing table to modify and alter the flow of packets in the network. Therefore, the integrity of the content of these messages must be guaranteed. This can be accomplished by using digital signatures and message digests.
- **Non-repudiation:** Routers cannot renounce ownership of routing protocol messages. A major alarm with the updates is the trust model associated with the propagation of updates that begin from distant nodes. Ad-hoc nodes obtain information from their neighbors and forward it to their other neighbors. These neighbors may advance it to other neighbors and so on.

In existing protocols, authenticity of updates generated only by next immediate nodes is verified by the adjacent nodes. In order to maintain trust associations, it becomes necessary to form a chain of routers (using signatures to protect integrity) and authenticate each one in turn, following the chain to the source. This is necessary because trust relationships are not transitive. Alternative solutions that circumvent chaining include the path attribute mechanism developed for Secure BGP and secure distance vector routing.

- **Confidentiality:** From perceptive the contents of packets, intermediate or non-trusted nodes are prevented sometimes as packets get exchanged between routers. Encrypting the routing protocol packets themselves can stop unauthorized users from reading it. Only routers that have the decryption key can decrypt these messages and participate in the routing. This is engaged when a node cannot trust one or more of its immediate neighbors to route packets properly, etc.

Each of these pleasing properties has a cost and performance penalty associated with it. Options like providing non-repudiation by chaining signatures and enforcing access control to routing tables using credentials are precisely valuable and unfeasible to implement and implement in a generalized routing protocol.

6. FRAMEWORK FOR SECURITY MEASUREMENT

This section presents the elements used in security and the structure of the Security Measurement framework is discussed here. This framework will be common to all. One can state his/her own view of security measure and assess the values of such measurement. The points which will be discussed in this framework are the components like computer security; “How to select units and scales for measurement; Estimation methodology and validity check for the measures.

Computer Security

Computer security is considered as a multi-dimensional attribute, and its correspondent dimensions are not surely equivalent properties. For example, a financial stock exchange network define security according to real time operations and search methods to tackle the problems come information privacy while an on-line newspaper just focus on the integrity of the information. To measure a multi-dimensional attribute is not an easy task. For this, prior identification of various phases of the attribute must be clearly defined.

Security is system dependent and must identify a set of important security-related attributes A decision also must be taken to judge the system representation of security system as a vector or a single value. For a single value, a model must be defined to relate the different attributes. For example, Standard of living can be measured by cost of everyday necessities, average salary level and the real estate prices, etc. In cases, measurements can be in form of a simple addition of the various ratings while a more refined model i.e. *weighted sum* is used to calculate the final

measure in other cases. Our framework presents a security measure by an *n* tuple which is of real numbers and each one is an aspect of the defined security. For example, As system security is union of three attributes i.e. confidentiality, integrity and availability, and a possible security metric is the three tuple:
<g1 (*confidentiality*),g2 (int*egrity*), g3 (*availability*) >
The values of this three-tuple specify the percentage measured strength of three attributes i.e. confidentiality, integrity and availability of the system. In a single measure, a formula is derived to give a single output by taking all the three inputs in form of confidentiality, integrity and availability.
For example, the tuple
<g1(confidentiality),g2(Integrity),g3(availability),f(g1,g2,g3)>
Where
f(g1,g2,g3)=
sum(g1(confidentiality),g2(Integrity),g3(availability))
sum(70% g1, 20% g2, 10% g3)
sum(0.65 g1 ,0.25 *g* 2 ,0.1 *g*3)
=0.70 g1 + 0.20 g2 + 0.10 g3

defines a measure in which confidential dependency is 70%, 20% system integrity, and 10% system availability.

A good measure starts with the prior knowledge of what to measure. The mandatory part is "How to select the relevant security properties". Future prospectus is to construct a set of guidelines to help researchers and practitioners understand and identify security-related concerns and translate them into specific security properties that will be measured later.

Units and Scales used
Different types of scales and units can be used in measuring attributes like confidentiality, Integrity and availability. E.g. Distance is measured in meters and kilometers; length in meters and centimeters; Temperature in Celsius and Kelvin.
Two purposes are solved using units and scales:
1. How to measure, and
2. How to interpret measured values.
Different interpretations are used for units and scales for different purposes.
1. Ordinal scale: This scale preserve or maintain the ordering among classes or categories. e.g. Mohs scale (used to check the hardness for minerals) [17].
2. Interval scales[17]: It maintains not only the ordering but also differentiate classes. E.g. Celsius and Fahrenheit scales.
3.Ratio scales[17]: With the maintenance of ordering as well as difference, it also keeps a look on ratio among classes. The Kelvin scale for temperature is a ratio scale [17].

The Estimation Methodology to measure security
In cases where direct measure is not possible to measure things, then a measuring instrument or an estimation method is used; e.g. Speed of light is used to measure distance between stars. It can be assumed as simple as to estimate person's age or as complex measuring distance between stars. The main thing is to select an appropriate estimation method that best approximates the real value. In computer security, direct measurements from end to end is not possible because of the scopes and structures of the modern computing systems. In these mentioned systems, security attributes are not only functions of a single entity but also functions of a host of objects and their interactions. To best approximate the security strength of large systems, an estimation method must be used.
There may be many estimation methods. For example, System reliability can be estimated by sampling the history of the entire system or by doing so on each component and integrate them in some manner. Though computer security estimation is difficult in large systems whereas it is easy to analyze small, standalone components of the system.

Basic Measurements
To measure the end-to-end security attributes of a complex system becomes an easy task if the ways to measure the security attributes of its basic components are clearly defined. This subsection explores "How to measure basic components". For this, units and scale types are used.
The security attributes such as confidentiality and integrity are defined as terms of qualities. In measuring such quality terms, an inherent difficulty is that there might be many different interpretations of what they actually mean. Therefore, "how these quality terms are to be defined" should be clearly interpreted. A model associated with the attribute to be measured should be defined. For example, confidentiality of information has always played a central role in computer security. Unauthorized disclosure of information, if not prevented, may cause catastrophic results. In general, the best solution to problem is to combine the good cryptography with physical security.
To describe confidentiality, a factor-criteria model called Confidentiality Model is shown below:

Attribute	Factors	Criteria
Confidentiality	1.Cryptographic Protection	a. Algorithm
		b. Keys and Secrets
	2.Physical Security	a. Physical media
		b. Accessibility
	3.Software Access Control	a. Effectiveness
		b. Reliability

Fig.5 Confidentiality Model

In figure 5, confidentiality is divided into three main factors: cryptographic protection, physical security and software access control which are then further divided into a set of lower level criteria in form of Physical media, Accessibility, Algorithm, Keys and secrets, Effectiveness and Reality. Some factors of this level of criteria can be easily and directly measured while others are still complex and need to be associated with a set of even lower level, directly measurable terms. For instance, Figure 6 shows cryptographic protection levels described by two criteria named as Algorithm and Keys and secrets; and four basic metrics named as Degree of testing, Implementation, Key Length and Key Storage.

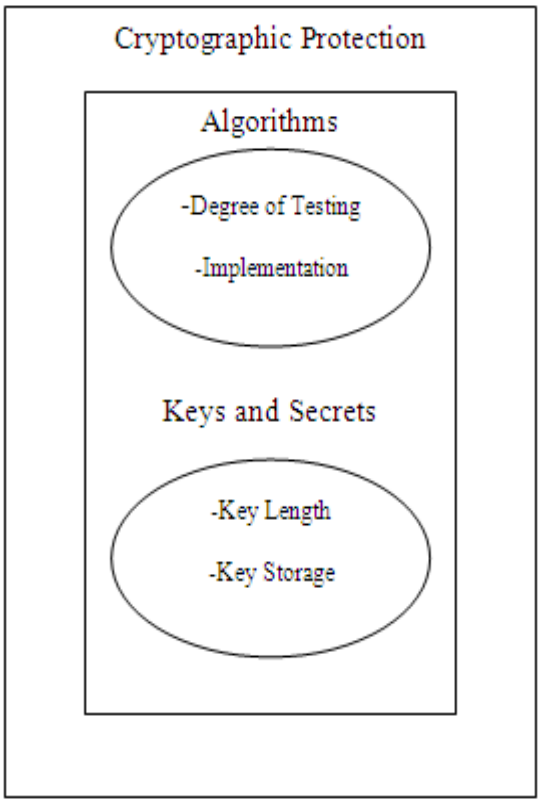

Fig.6 Cryptographic Protection

A list of questions is used to get the information about in how much strict manner, the algorithm is tested; how long it has been used and what technique of cryptoanalysis was carried out against it. Similar list is used to evaluate the algorithm implementation and the key storage mechanism. Various methods are used to convert this list into a metric. First method is to use closed questions. The form of questions will be in 'Yes' or 'No'. To a 'Yes' answer 1 will be assigned and 0 for 'No' answer. The whole measure will be derived by calculating the percentage 'Yes' questions. The computed value of cryptographic protection level will be between 0 and 1.

=½(1/2(Number of 1s for degree of testing/Total Number of questions + Number of 1s for implementation/Total number of questions) + 1/2(Key Length/Minimum Length infeasible to break+ (Number of 1s for key Storage/Total Number of questions))

The equivalent measures can be calculated for physical security and software access control. Finally, "confidentiality" is measured by taking the mean of previously defined three measures

Confidentiality = (sum (measure for physical security+ cryptographic protection+ access control))/3

Focus should be on to implement these metrics because the overall estimate dependency is on the basic metrics. To reduce the chance of misinterpretation, all the diagrams, mathematical equations, or questionnaires must be clearly specified. Defects must be looked upon. Lastly, they should integrate what is important to the organization or experts' needs.

In the above example, same weight is used for all the questions and factors. In special priorities, different weights should be used. Models can be outlined in many different forms. For descriptive purposes, some models are outlined here for different representations. For common cases, a set of general models will be developed. No one is forced to accept any of the models described above in their analysis. Everyone can develop the model according to their specific requirement. We just focus to accommodate the basic principles in Security Measurement framework for such model.

Integrity: The integrity model is very much similar to the confidentiality model e.g. Key, Factor and lower level criteria. Integrity Model is shown in following figure. It has three components:
Physical Security, Cryptographic protection and Access control.

Attribute	Factors	Criteria
Integrity	1.Cryptographic Protection	a. Algorithm
		b. Keys and Secrets
	2.Physical Security	a. Physical media
		b. Accessibility
	3. Access Control	a. Effectiveness
		b. Reliability

Fig.7 Integrity Model

Different questions may be used to assess the criteria in order
to reflect unique integrity concerns.

Availability: In opposition of unfavourable services, Real time operations causes disastrous results.
For example, Regular strokes given intentionally or an attack occasionally; if both leads to death, then what is the difference between two. How can both will be differentiated as Intentional malicious bombardment in the network and cheap performance caused by random overloading?
To answer all the questions is a tedious task. Proposal is to review the subject through fact finding methods or experimental measurement and discover its characteristic behaviours. A measurable formula for Availability is shown below:

Availability = the probability to achieve demand request

This probability can be resolved by using some methods like statistics over a period of time, samplings or specific testing. To reduce the effects of extreme and random events, probabilistic measures are used. Note that a maximum turnaround time should be declared for service requests.

Non-repudiation: With the speed of E-commerce, Non-repudiation has become an important concept. Appropriate procedure must be provided to assist Non-Repudiation for security operations
. Non-repudiation model is shown in following figure:

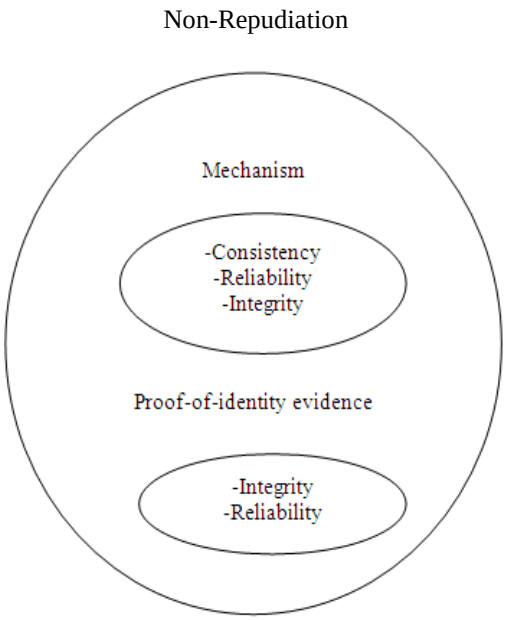

Fig.8 Non-Repudiation Model

A suitable proof-of-identify evidence and a tough underlying mechanism is used for Non-repudiation. For example, a four digit ATM PIN is used as identity-proof, in some cases, this identity-proof also fails in security operations then biometric data in form of finger prints and physical signatures are used. Integrity , consistency and reliability issues must also be considered.

***Authentication*:** Authentication becomes mandatory for latest computer systems, Successful authentication is the basis for security services. Authentication Model is described in Figure 9.

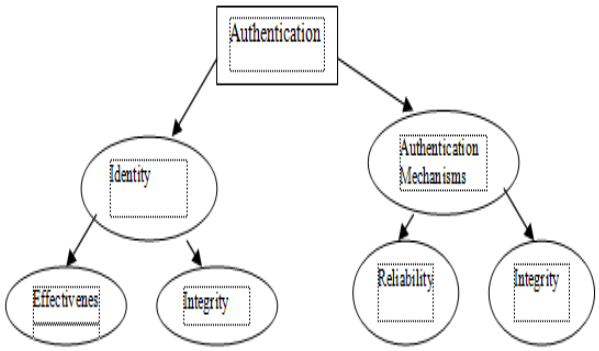

Fig.9 Authentication Model

Models for High level secured attributes have to be defined which depends on non secured attributes.

Validate the measures

The measurements described previously should be "valid" for optimal security operations. The theory or statements considered as basis does not infringe the measurement theory. For validation, observed behaviours or relations can be used. validate our measures. To prove or disprove the formulas, experimental theory must be used.

7. CONCLUSION

The concept of a security measurement technique is proposed in this paper. The framework only gives the theoretical knowledge "How to measure Security." No practical implementation is shown in this paper. Though this study is a step toward the right direction, but without any proof. Knowledge can be extended by studying this paper. In next paper, we will prove all these theories with proof by experimental set up.

REFERENCES

[1] Djamel DJENOURIx, Nadjib BADACHEz A Survey on Security Issues in Mobile Ad hoc Networks

[2] IEEE Computer Society, "IEEE 802.11 Standard, IEEE Standard for InformationTechnology",1999. http://standards.ieee.org/catalog/olis/lanman.html.

[3] S Corson and J. Macker. Mobile Ad hoc Networking (MANET):Routing Protocol Performance Issues and Evaluation Considerations. Internet Request for comment RFC 2501, Jan 1999.

[4] Michael Jarrett, Paul Ward, "Trusted Computing for Protecting Ad-hoc Routing," cnsr, pp. 61-68, 4th Annual Communication Networks and Services Research Conference (CNSR'06), 2006.

[5] Muhammad O Pervaiz, Mihaela Cardei and Jei Wu: Routing security in ad hoc wireless networks, Department of Computer Science and Engg, Florida Atlantic University, Boca Raton, FL 33431.

[6] C. Perkins and P Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing DSDV for mobile computers". In ACM SIGCOMM'94 Conference on Communication Architectures, protocols and applications, 1994, pp. 234-244.

[7] C.E. Perkins, E. Belding Royer, and S.R. Das, "Ad hoc On demand distance vector (AODV) routing", IETF RFC 3561, July 2003.

[8] Hao Yang, Haiyun Loo, Fan Ye, Sogwu Lu and Lixia Zhog: Security in mobile ad hoc networks, challenges solution, Wireless communication, IEEE Volume I, issue I publication date Feb 2004.

[9] Priyanka Goyal1, Vinti Parmar2, Rahul Rishi3 "MANET: Vulnerabilities, Challenges, Attacks, Application" IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893

[10] Rusha Nandy, Debdutta Barman Roy "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme " Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)

[11] T Friiso, T Brekne, P Haaland, M Radziwill. Security challenges in self organizing wireless networks. Telenor No ISBN 82-423-0581-1, ISSN 1500-2616, project No TFPFAN programme peer to peer computing security Gr, Dec 2003.09.08.

[12] Project No: IST-507102, Project full title: My Personal AdaptiveGlobalNETMAGNET).http://www.istmagnet.org/GetAsset.action?contentId=942902&assetId=943011

[13] Rachika Gupta et al./ Indian Journal of Computer Science and Engineering (IJCSE) ISSN : 0976-5166 Vol. 2 No. 5 Oct-Nov 2011 741

[14] D. B. Johnson, D. A. Maltz, " Dynamic source routing in ad-hoc wireless networks," Mobile Computing, 1996.

[15] W. Stallings," Network and Internetwork Security Principles and Practice", Prentice Hall, Englewood Cliffs, NJ, 1995.

[16] NIST, Fed. Inf. Proc. Standards, "Secure Hash Standard," Pub. 180, May 1993.

[17] F. Roberts, "Measurement Theory, with Applications to Decision-Making, Utility, and the Social Sciences", Addison-Wesley, 1979.

[18] http://ids.nic.in/tnl_jces_Jun_2011/PDF/pdf/.%20secure%20routing%20protocols%20in%20adhoc%20networks.pdf

[19] https://waset.org/Publication/addressing-security-concerns-of-data-exchange-in-aodv-protocol/8591.