ROLE OF TRUST IN PROVIDING INTEGRATED SECURITY SOLUTION FOR MOBILE AD-HOC NETWORKS

1st Renu, 2nd Dr.Sanjeev Sharma
[1]Research Scholar, [2]Professor and HOD
[1,2]School of Information Technology,
[1,2]RGPV, Bhopal, India

Abstract : In MANETs, mobile devices can communicate with each other without any predefined infrastructure.This attracted feature makes it very popular these days in various application areas.In constrained resources environment, the nodes communicate with each other based on assumption of cooperation . Cooperation related security issues cannot be addressed through traditional approach, because they can change the behavior of MANET node. Trust can play key role for all cooperative actions in MANET. An efficient trust management mechanism should be developed in order to verify the identities on the ad hoc networks for reliable communication. In this paper we discuss the concepts and properties of trust and derive various dimensions of security as well as trust with the intention to fill the gap of earlier surveys. The paper covered all previous trust management schemes for data protection, secure routing and other network activities with their unique features, merits and demerits.

INDEX TERMS - SECURITY,ROUTING,TRUST MANAGEMENT, MOBILE AD HOC NETWORKS, TRUST,CRYPTOGRAPHY

I. INTRODUCTION

Trust is very useful tools that can provide security solution in challenging environment of communication like MANET.It is commonly assumed that all devices are cooperative and trustworthy.This acssumption open the door for attackers and malicious nodes can make use of this to corrupt the network. A lot of attacks such as man-in-the-middle, black hole, DOS may be deployed to destroy the network. In MANET trust can be represented according to the behavior of nodes (or entities, agents etc)[2].The probability value of trust varying from 0 to1, where 0 represent DISTRUST and 1represents TRUST [3].There are so many surveys existing but no one included the major challenge that is high mobility of MANETs where nodes continuously join and leave the networks [11] having constraints resources. In this paper "trust" with the correlation of risk is defined, some popular attacks are discussed and also shown that how trust can work against these vulnerabilities to make the MANET secured. Various existing trust management schemes involved in major areas like routing and group communication and key management, are investigated with their merits and demerits & findings. In spite of the existing surveys on trust, there was a gap for a more comprehensive and up-to-date survey to recent trust models. Here some more dimensions and techniques have been exposed and existing surveys did not cover them.

The rest of the paper is organized as follows: Section 2 presents potential attacks and how they can be countered by trust model. Section 3 describes scope of the Trust for securing MANET also includes the review of trust based models for key management and secure routing and Section 4 describes Classification of Trust based system . Section 5 covers the discussion and at last section 6 concludes the paper.

1.1Trust general

In real world while making decision, people normally trust the person they know personally and/or have known from someone else. They trust them till they are in a good relation with them. So how much trust a person can have on other is a relative term, if he is in communication with the person than it is supposed to be trustworthy otherwise not.Trust plays an important role in our social life, especially in business environments, or when financial issues are involved [6]. Apparently, trust is a key of cooperative human actions as a mechanism of economic choice and risk management. The definitions of trust can be classified based on the consideration of structural, disposition, attitude, feeling, expectancy, belief, intention, and behavior. Thereby various definitions of trust is found in the literature [9,10]. Networks are revolutionizing the way we conduct our personal and organizational business, and the human notion of trust has been extended into the digital world. In digital world or virtual societies the goal of the research on trust is to increase the reliability and performance of electronic communities [10].

1.2 Definition of Trust: Trust can be defined in so many ways by so many different researchers across disciplines that a typology of the various types of trust is sorely needed. Trust can be seen as the confidence, belief, and expectation regarding the reliability, integrity, ability, and other characteristics of an entity [4] Trust is the lubricant that supports relationships and makes a network work equation.

1.3Relation between Trust and Risk:

Trust can be considered as a tool to cover the risks as shown below:

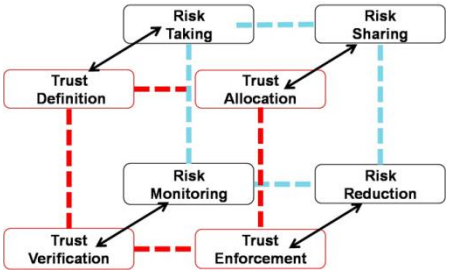

Fig: 1 A relation betweenTrust and risk

Having different definitions in computing literature "trust" is considered as followed in this paper: "the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trust or, irrespective to the ability to monitor or control that other party"{4}.

1.4 Need of Trust :

In all networks a valid, secure, optimal communication is needed. As we all familiar with the behaviour of nodes in the MANET that is unpredictable, frequent and random in nature; the nodes can leave or join the network To find this kind of path cooperation of intermediate nodes plays a vital role. In MANET cooperation of nodes is required when a node wants to communicate with a node that is out of its range ,without cooperation of nodes it would be never possible to communicate.Trust can paly a vital role to provide the cooperation towards a secured communication.Every security system depends on trust, in one form or another, among users of the system. In general, different forms of trust exist to address different types of problems and mitigate risk in certain conditions during communication.

1.5 Properties of Trust

Trust mechanism is introduced in the protocols to provide security in MANET. Trust is a value that is calculated on the basis of nodes action when needed. Trust is introduced to prevent from various attacks like wormhole, black-hole, Dos, selfish attack etc. Trust can be implemented in various ways such as by reputation, subjective logic, from opinion of nodes etc as there are no particular definitions of trust. According to (MarcBranchaud, Scott Flinn) trust relationships are applicable only in some specific context which may asymmetric and it depends on the uncertainty of nodes action.If node A trusts B and node B trust C that does not mean that A trusts C. Trust can be summarized as:

- Trust is earned, not bestowed or forced
- We must safeguard trust to ensure that autonomy is not abused in a network.
- Trust builds living networks that are highly resilient, flexible and efficient.
- trust is remaining open in the face of vulnerability

1.6 Trust Representation:

Trust can be represented as either continuous or discrete numbers.In continuous, trust values are represented as "V.High", "High", "Mid" and"Low" which are in a decreasing order of trust. In discrete, the trust value is a continuous real number in [-1, +1] where -1 denotes completely no trust, 0 complete uncertainty, +1 complete trust respectively.

2. POPULAR ATTACKS: In our earlier paper[7]We presented some typical and dangerous vulnerabilities in the mobile ad-hoc networks. Trust is introduced to prevent from various attacks like wormhole, black-hole, Dos, selfish attack etc.Now we will investigate that how these vulnerabilities can be handled using trust based models.

2.1 Sybil attack : In the Sybil attack [4]a malicious node behaves as if it were a larger number of nodes (instead of one) by impersonating other nodes or simply by claiming false identities. In the worst case, a Sybil attacker may generate an arbitrary number of additional node identities, using only one physical device. V. Sujatha and E. A. Mary Anita proposed an efficient trust based method for detecting Sybil nodes in a dynamic sensor network[]. They included location of the node, timestamp of the message and trust value for detecting the Sybil node. R. Naveen Kumar V. Bapuji Dr. A. Govardhan etc presented DAS, a novel decentralized protocol that limits the corruptive influence of Sybil attacks, including Sybil attacks exploiting IP harvesting and even some Sybil attacks launched from botnets outside the system.

2.2. SYN flooding It is a type of attack done by the attacker to a specific server to down them by flooding the requests. So, the server will be busy waiting for the requests created by the attacker.. If sufficient connections are established among multiplesenders and the victim, it is likely that its memory resources may be exhausted (table overflow), owing to the currently open connections and the victim cannot now accept a new legitimate request for a connection. Meka, Virendra, and Upadhyaya gave Trust based routing decisions in mobile ad-hoc networks in 2006.

2.3. Jamming :This type of DoS attack is initiated by a malicious node after determining the frequency of communication used by the receiver and using the same frequency to send data to the receiver thereby interfering with its operation.

2.4. packet drop attack / blackhole attack: In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This usually occurs from a router becoming compromised from a number of different causes.In a flooding-based protocol, the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply consisting of an extremely short route. If the malicious reply reaches the requesting node before the reply from the actual node, a forged route gets created .Mahamuni and others(2016)[35] addresed BLACKHOLE Attacks by giving Trusty DSR Protocol for MANET .

2.5. Gray Hole Attack :Here packets are mislead in the network by agreeing to forward the packets in the network. The malicious behavior of gray hole attack is very different It drops packets while forwarding them in the network. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behaviour

2.6 Wormhole attack: In this attack, an attacker receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network, and from there the packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through a single long range wireless link or even through a wired link between the two colluding attackers. Owing to the broadcast nature of the radio channel, the attacker can create a wormhole even for packets not addressed to itself.If wormholes are created purely for packet relaying purposes, then wormholes are harmless, provided theattacker has no malicious intentions.

3. PREVIOUS TRUST BASED WORK FOR SECURING MANET:

Employing cryptography in MANET are quite impractical because involved nodes have limited resource and Open to several attacks. Trust mechanism is used as an alternative to maintain trustable network environment. According to Golybeck [4] trust has three basic properties: Transitivity,Asymmetry and personal opinion. Comparitively trust model in ad-hoc network is better because it gains higher security level and improves efficiency in network. The trust based security protocol attains confidentiality and authentication of packets in both routing and link layers of MANETs.

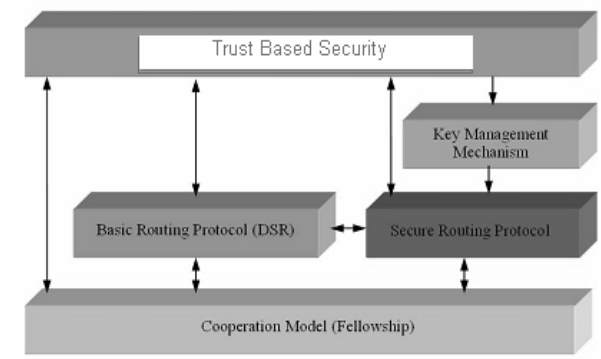

Fig2 :Layered architecture of trust based security

Availability of network services, confidentiality and integrity of the data can be achieved by addressing two main areas related to security in MANET

3.1 Trust based Group communication and Key management:

Secure group communication became the basic requirement in many group oriented applications of mobile ad hoc network (MANET). In order to enhance the privacy among group members, proper group key management schemes can be used to encrypt and decrypt the payload. This section will investigate existing key management schemes for mobile ad-hoc network to achieve the security and trustworthiness

Key management can be either Centralized or distributed.In a centralized system, a single entity is responsible to carry out group communication. Key generation, distribution and management are all carried over by this entity. Scalability overhead, Storage overhead and Single point of failure are some limitations ,which makes it unsuitable for MANET. Idea behind Decentralized Group Key Management scheme is to reduce the load on KDC, the central entity. This is achieved by splitting the group members into several subgroups and each subgroup is managed by its own subgroup controller. This approach solves the problem of a single point failure.Threshold key management scheme was proposed in which certification services are distributed among 'n' serving nodes(H.Zhou .,1999).Each serving node generates partial certificate. To generate secret key, any node must have 'n' partial certificates. serving node must maintain public key of all other nodes in network, which requires more memory and also suffers from lack of certificate revocation mechanism .

In network security, direct trust is required when individuals from separate CA domains (not cross-certified) exchange keying information.The Concept of Trust in Network Security came to secure their communications which is ccoperation based here the users must trust each other on a personal basis. Without personal trust in this scenario, exchanging keying information is of no value because the keying information itself should not be trusted. When direct trust is applied to secure communications, it is solely the responsibility of each of the parties to ensure that they are comfortable with their level of personal trust.Finally, we need a self-organized, key distribution system that allows users to generate their public-privatekeypairs. Digital signature and public key encryption mechanisms require a key management service to keep track of key and node binding and assist the establishment of mutual authentication between communication nodes. Traditionally, the key management service is based on a trusted entity called a certificate authority (CA) to issue public key certificate of every node. The trusted CA is required to be online in many cases to support public key revocation and renewal. But it is dangerous to set up a key management service using a single CA in an ad hoc network. It will be the vulnerable point of the network. If the CA is compromised, the security of the entire network is crashed. In [2] and [16], threshold cryptography is used to provide robust and ubiquitous security support for the ad hoc networks. The CA functions are distributed through a threshold secret sharing mechanism. This approach is very complicated to implement. It is also hard to survive from multiple hijacked nodes that have secret shares. In this scenario trust can be better solution. The security for the ad hoc networks is still in its infancy. Existing solutions cannot solve this issue well. What is missed is an effective mechanism that can provide reasonable inference based on available knowledge, such as intrusion detection result, past experience, communication data value, and preferences, to evaluate trust relationship among network nodes. With the evaluation result, it is possible to make correct decision or close-correct decision on security protection. New mechanisms are expected to adapt the special characteristics of the new network paradigm

3.2 Trust based Secure routing proposals in MANET's

Trust based routing protocols have great demand and researchers trying out many variations of them.The Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network.Some of the important features of AODV are

- ✓ Nodes keep record of only needed routes
- ✓ Broadcasting is minimized
- ✓ Reduces memory and less duplications
- ✓ Instant reports to link breakage inactive routes
- ✓ Loop free routes maintained
- ✓ large populations of nodes can be addressed

There are quite a lot of work have presented on this topic .Sharma, S., Mishra, R.etc proposed trust based security approach by maintaing a special data stucture called trust table in 2010 [9].Sridhar, S., & Baskaran, R. (2015)[10]proposed (TS-AODV)in this the routing information will be transmitted depending upon highest trust value among all on level of trust factor.Dr. K. Prasadh utilized Trust Evaluation Factor. Each snode has k trust evaluation matrices which has many trust evaluation factors like Link quality,Distance,Mobility etc[11].A.Menaka Pushpa modified existing AODV routing protocol in order to adapt the trust based communication feature. Proposed trust based routing protocol is equally concentrates both in node trust and route trust[12].Light-weight trust-based routing protocol is proposed for mobileadhocnetworks by N. Marchang1R. Datta which consumes limited computational resource and suitable for blackhole attack and the grey hole attack[13].Durgesh Wadbude etal. [14] proposed an efficient secure AODV routing protocol which allows authentication of AODV routing data. Hash chains, Digital Signature and Protocol Enforcement Mechanism to secure packets in AODV. Hash Chain is used to secure the Hop count. SAODV includes another feature which allows intermediatenodes to reply to RREQ message.Secure aware ad hoc routing (SAR) in [15] uses security properties (e.g. time stamp, sequence number, authentication password or certificate, integrity, confidentiality, and non-repudiation) as a negotiable metric to discover secure routes in an ad hoc network. The SAR can be implemented based on any on-demand ad hoc routing protocol with suitable modification. But it only considers the effect of security properties on the trust.In [18], a set of design techniques for intrusion resistant ad hoc routing algorithm (TIARA) was presented mainly to against denial-of-service attacks . Commonly, it is interpreted as reputation, trusting opinion and probability [4]. Simply, we can consider it as the probability that an entity performs an action as demanded.HarrisSimaremare et al.[17] proposed AODV routing protocol based on trust mechanism using the concept of local trust and global trust. Local trust is based on total received packet and total forwarded packet with reference to specific nodes whereas Global trust is based on total number of packets received and total number of packets forwarded in network. Trust based Ad hoc On-Demand Routing protocol was presented the algorithm works on the concept of honest value calculated on a concept of hop/trust to protect networks from malicious nodesby Gupta & Pandey [36] algorithm works on the concept of honest value calculated on a concept of hop/trust to protect networks from malicious nodes.In ad hoc networks, securing routing protocols is one of the fundamental challenges. Summery of all previous work in this area is depicted in the below table.

Table 1: Trust based Contributions for secured AODV

Author	contribution	Features
R. S. Mangrulkar Mohammad Atique [2010]	Trust based secured adhoc On demand Distance Vector Routing protocol for mobile adhoc network	Adds a field in REQ which stores trust value indicating node trust and routing information will be transmitted depending upon highest trust value among all.
DR. K. PRASADH[2014]	TRUST BASED AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL AGAINST WORMHOLE ATTACK	HAVAL hash function is used with simple iteration of compression function. HELLO packet are modified
Priya Sethuraman N. Kannan	Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET	Bayesian probability is introduced which consumes low energy
A.Menaka Pushpa	Trust based secure routing in AODV routing protocol	modified AODV in order to adapt the trust based communication and equally concentrates both in node trust and route trust.
N. Marchang1R. Datta	Light-weight trust-based routing protocol for mobileadhocnetworks	Addressed two kinds of attacks, blackhole attack and grey hole attack.Evaluation using both self-trust and neighbour trust
Durgesh Wadbude etal.	Secure Ad-hoc On Demand Distance Vector Routing	Hash chains, Digital Signature and Protocol Enforcement Mechanism to secure packets in AODV
HarrisSimaremare et al	Secure AODV Routing Protocol based on Trust Mechanism	concept of local trust and global trust.Blackhole attack and Dos attack

A secure routing solution is proposed by so many researchers But unfortunately, no one solve the problem caused by cooperation of multiple malicious nodes.While many secure routing schemes focus on preventing attackers from entering the network through secure key distribution or authentication and secure neighbor discovery, trust management can guard routing even if malicious nodes have gained access to the network.

4. CLASSIFICATION OF TRUST EVALUATION SCHEMES:

There is a need for trust evaluation in different networks like ad hoc networks, e-commerce applications, service oriented computing, and multi-agent systems which have different focuses. Different researchers contributed and presented various model to compute the trust.There are different trust evaluation methods for different types of applications and trust measures

Table 2: Comparision of trust evaluation methods

Model	Recent contribution	Basic working	Commmu	Features	Merits	Application
Simple Summation	Wang and Varadharajan	sum the number of positive and negative ratings	Direct	Sum and average method can be combined with weighted summetion	Simplicity and Scalability	Small and large scale of ad-hoc network
Fuzzy Model	Manchala Sabater & Sierra	membership functions are used	Direct	Fuzzy functions and wights decision	Self organized	Small and large scale of ad-hoc network
Cluster Based	Rutvij H. Jhaveri, Narendra M. Patel and	Ad-hoc network is divided into clusters	Hierarical	Zone routing protocol is used	no need of personal and past experiences	Only for small scale of MANET
Maturity Based	A. Josang	Concept of Maturity is introduced for MANET	Indirect	trust increases between people as time goes by, same	robust and accurate	Small and large scale of ad-hoc network
PKI Based	Janani V S and Manikandan	Concept of Public Key Infrastructu re	Certificates	certificate revocation	having less maintenance overhead	Small and large scale of ad-hoc network
Hybrid approach	Antesar M Shabut, M. Shamim Kaiser, etc	A multidimensional trust evaluation	Hybrid	All aspects affected to trust are covered	Dishonest trust computaipon is handled	Small and large scale of ad-hoc network

In This area researcher like Ramana K.Seshadri, Chari A.A., Kasiviswanth N[25] and Antesar M. Shabut, M. Shamim Kaiser, Keshav P. Dahal, Wenbing Chen contributed a lot still it is not realistic to look for one all-round perfect solution that fits all fields. We can choose suitable features from multiple model to design the solution for our area.

5.FURTHER DISCUSSION:

The ad hoc networks are dynamic by nature, they require a dynamic security solution that fits this fundamental characteristic. The paper tries to explore the importance of social believe procedure on decision-making and introduces it into the ad hoc networks. The perfect security solution is hard to achieve but two challenging actions group key management and secure routing can be shielded to reduce security threats.

6. CONCLUSION AND FUTURE WORK:

Trust is simple approach to security based on the mutual trust and behaviour grading and past experience .It is effective against a pool of common attacks and feasible with respect to the architectural demand of MANET. The paper covered various aspects of trust including its goals, properties, representation, and classification of various model along with their strength and weaknesses. A comprehensive review of some important research works focusing on trust- for both key management and secure routing is presented in this paper . Trust based schemes are Attack-tolerant ,Cooperative ,Flexible ,Lightweight and Scalable as well as Compatible to the rapidly growing network size .Finally, some open problems that are being currently investigated in this domain are also discussed.

REFERENCES

[1] R. J. Lewicki and B. B. Bunker, “Trust in Relationships: A Model of Trust Development and Decline, In Conflict, Cooperation and Justice, B. Z. Rubin, Ed. San Francisco: Jossey-Bass, 1995, pp. 133-173.

[2] D. H. McKnight, V. Choudhury, and C. Kacmar, “Developing and Validating Trust Measures for e-Commerce: An Integrating Typology, Information Systems Research, Vol. 13, pp. 334-359, 2002

[3] Raju Barskar* and Meenu Chawla”A Survey on Efficient Group Key Management Schemes in Wireless Networks” Indian Journal of Science and Technology, Vol 9(14), DOI: 10.17485/ijst/2016/v9i14/87972, April 2016

[4] D. Gefen, E. Karahanna, and D. W. Straub, “Trust and TAM in Online Shopping: An Integrated Model, MIS Quarterly, Vol. 27, pp. 51-90, 2003.

[5] P. Dasgupta, “Trust as a Commodity. In Trust, D. G. Gamretta, Ed. New York: Basil Blackwell, 1988, pp. 49-72.

[6] S. Ba and P. A. Pavlou, "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior, MIS Quarterly, Vol. 26, pp. 243-268, 2002.
[7] RENUMISHRA,DR. SANJEEV SHARMA,DR. RAJEEV AGRAWAL" Vulnerabilities and security for ad-hoc networks" Proc.IEEE International Conference on Networking and Information Technology Page no.192-196 April 2010
[8] D. H. McKnight, L. L. Cummings, and N. L. Chervany, "Initial Trust Formation in New Organization Relationships, Academy of Management Review, Vol. 23, pp. 473-490, 1998
[9] Sharma, S., Mishra, R., & Kaur, I. (2010). New trust based security approach for ad-hoc networks. 2010 3rd International Conference on Computer Science and Information Technology, 9, 428-431.
[10]Sridhar, S., & Baskaran, R. (2015). Efficient Routing in Mobile Adhoc Networks Emphasizing Quality of Service by Trust & Energy based AODV.
[11] .n satheesh, 2 dr. K. Prasadh"Trust based ad hoc on demand distance vector routing protocol against wormhole attack" Journal of Theoretical and Applied Information Technology 31st December 2014. Vol.70 No.3
[12]Pushpa, A.Menaka. (2010). Trust based secure routing in AODV routing protocol. 1 - 6. 10.1109/IMSAA.2009.5439454.
[13]N. Marchang1R. Datta"Light-weight trust-based routing protocol for mobileadhocnetworks" Published in IET Information SecurityReceived on 7th July 2010Revised on 25th May 2011doi:10.1049/iet-ifs.2010.0160
[14]Wadbude, Durgesh, and Vineet Richariya."An Efficient Secure AODV Routing Protocol in MANET." International Journal ofEngineering and Innovative Technology(IJEIT),vol.1, pp.274-279, April 2012
[15] Yi, Seung & Naldurg, Prasad & Kravets, Robin. (2001). Security-Aware ad-hoc routing for wireless networks. Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing: MobiHoc 2001.
[16] Meka, Virendra, and Upadhyaya, "Trust based routing decisions in mobile ad-hoc networks" In Proceedings of the Workshop on Secure Knowledge Management, 2006.
[17] Shabina Parbin ; Leeladhar Mahor" Analysis and prevention of wormhole attack using trust and reputation management scheme in MANET
[18] Ramanujan, Ranga & Kudige, S & Nguyen, T. (2003). Techniques for intrusion-resistant ad hoc routing algorithms (TIARA). 98 - 100 vol.2. 10.1109/DISCEX.2003.1194934.
[19]Seung Yi, Prasad Naldurg, Robin Kravet. Security-awarahoc routing for wireless networks. http://www.cs.uiuc.edu/Dienst/Repository/2.0/Body/ncstrl.uiu
[20]Jiejun-K, Petros-Z, Haiyun-Luo, Songwu-Lu, Lixia-Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. Proceedings Ninth International Conference on Network Protocols. ICNP 2001, Riverside, CA, USA, Nov. 2001
[21]McKnight, D. Harrison, Chervany Norman L. What is Trust? A Conceptual Analysis and An Interdisciplinary Model. In Proceedings of the 2000 Americas Conference on Information Systems (AMCI2000).
[22]Ramanujan-R, Ahamad-A, Bonney-J, Hagelstrom-R, Thurber-K. Techniques for intrusionresistant ad hoc routing algorithms (TIARA). Proceedings of IEEE MilitaryCommunications Conference (MILCOM'00), vol.2, Los Angeles, CA, USA, Oct. 2000.
[23]McKnight, D. Harrison, Chervany Norman L. What is Trust? A Conceptual Analysis and An Interdisciplinary Model. In Proceedings of the 2000 Americas Conference on Information Systems (AMCI2000). AIS, Long Beach, CA, August 2000..
[24]Janani V S and Manikandan "Efficient trust management with Bayesian-Evidence theorem to secure public key infrastructure-based mobile ad hoc networks EURASIP Journal on Wireless Communications and Networking2018
[25]Ramana K.Seshadri, Chari A.A., Kasiviswanth N., "A Survey On Trust Management For Mobile Ad Hoc Networks," International Journal of Network Security & Its Applications, Volume 2, Number 2, pp. 75-85, April2010
[26]Prasadh, D.K. (2014). Trust based ad hoc on demand distance vector routing protocol against wormhole attack.
[27]Wadbude, Durgesh, and Vineet Richariya."An Efficient Secure AODV Routing Protocol in MANET." International Journal ofEngineering and Innovative Technology(IJEIT),vol.1, pp.274-279, April 2012
[28]HongMei Deng, Wei Li, Dharma P. Agrawal. RoutingSecurity in Wireless Ad Hoc Networks. IEEE Communications Magazine, October 2002, p70-75.
[29]Meka, Virendra, and Upadhyaya, "Trust based routing decisions in mobile ad-hoc networks" In Proceedings of the Workshop on Secure Knowledge Management, 2006.
[30]Dr.A.l.narasimha rao Inderpreet kaur Renu Mishra"Composite key management scheme using neurofuzzy logic"Conference RGPV,Bhopal
[31]Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis "Secure Routing and Intrusion Detection in Ad Hoc Networks" Third IEEE International Conference on Pervasive Computing and Communications, 2005.
[32]V. Sujatha and E. A. Mary Anita" An efficient trust based method for Sybil node detection in mobile wireless sensor network" AIP Conference Proceedings 2016
[33]R. Naveen Kumar1* V. Bapuji1 Dr. A. Govardhan2 Prof. S.S.V.N. Sarma3 An Improvement to Trust Based Cross-Layer Security Protocol against Sybil Attacks (DAS) "Computer Engineering and Intelligent Systems www.iiste.org ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
[34]Shiqun Li, Tieyan Li, Xinkai Wang, Jianying Zhou andKefei Chen "Efficient Link Layer Security Scheme for Wireless Sensor Networks" Journal of Information And Computational Science, Vol.4, No.2,pp. 553-567,June 2007
[35]Mahamuni (2016). Trusty DSR Protocol for MANET To Mitigate BLACKHOLE Attacks.International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 5 (2016) pp 3083-3091
[35] Gupta, N. K., and Pandey, K. (2013, August), "Trust based Ad-hoc on Demand Routing protocol for MANET". In Contemporary Computing (IC3), 2013 Sixth International Conference on (pp. 225-231). IEEE.
[36] Simaremare, H., Abouaissa, A., Sari, R. F., & Lorenz, P. "Secure AODV Routing Protocol Based on Trust Mechanism." In Wireless Networks and Security,Springer Berlin Heidelberg, pp. 81-105, 2013
[37] H. Liang, Y. Xue, K. Laosenthakul, and S. J. Lloyd, "Information Systems and Health Care: Trust, Uncertainty, and Online Prescription Filling, Communications of AIS, Vol. 15, pp. 41-60, 2005