ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

Energy Efficient Routing Protocol for Mobile Ad hoc Networks using Trust Based Security

Vemana Chary. D[1], Padmanabham. P[2], Prabhakara Rao. B[3]

Associate Professor, Department of ECE, Bharat Institute of Engineering & Technology ,Hyderabad, India[1]

Professor& Director of Academics, Department of CSE, Bharat Institute of Engineering & Technology,Hyderabad, India[2]

Professor , Department of ECE, University college of Engineering, JNTUK, Kakinada, India[3]

Abstract--MANET is a well known network in which wireless nodes are connected. This is also known as infrastructure less network. MANET might have colluding nodes in the network environment. The colluding nodes cause internal attacks in the wireless network. These results in security problems in the network and finally the MANET performance will go down or even the network breaks down. To overcome this problem, this paper presents mechanisms to detect colluding nodes and defend them. The proposed algorithm works on route detection trust management for the purpose of detecting colluding nodes and defending them from causing internal attacks. The local forwarding nodes discover routes and also involved in calculating trust. In order to calculate trust value of each nodes the trust of its one – hop neighbors is calculated. In cluster heads the information such as trust and route discovery is stored and maintained. The simulation results revealed that the proposed algorithm is effective in secure routing in MANETs.

Keywords – MANETs, trust, broadcasting, colluding nodes

I. INTRODUCTION

MANET is a wireless network that is having no fixed infrastructure. It is a set of mobile devices that can communicate to each other without having cabled network. They also do not need help from network infrastructure for the purpose of communication. There are many real world applications that use Mobile Ad Hoc Networks. Some of them include battlefield applications, rescue work applications, civilian applications like outdoor meeting, money transfers, and ad-hoc classrooms. There are many advantages of ad hoc networks. However, they also throw security challenges. The security attacks might be internal or external attacks. The internal attacks are generally caused by the colluding nodes in the MANETs. Mobile ad hoc network is made up of nodes that are self contained and having ability to connect to nearby wireless node and configure them without having dependency on any pre-defined network infrastructure. Fraudulent activities are done by one or more colluding nodes that work together. The colluding nodes try to hide their activities in order to keep their misbehavior remain hidden. Thus the colluding nodes compromise one or more nodes in the network so as to perform fraudulent activities and cause problems in the networks with their internal attacks. The main internal attacks they cause include resource consumption attack, fabrication attack, replay attack and black hold attack. In MANETs, for resource management a cluster is formed that is a set of computers interlinked. These clusters are formed based on the radio range of nodes. In MANETs a cluster-based communication infrastructure is used for broadcasting. It also reduces collision in networking, energy consumption, and delay in packet transmission. It also improves throughput of the network [3], performance of features such as limited bandwidth usage, virtual circuit support and power consumption.

In case of pure ad hoc networks, trust management becomes very complicated by central authority and other nodes in the MANET and their inter-dependency. It is very challenging to have trusts calculated from different levels [6]. For ambiguity reasoning a method is proposed in [16]. The name of the method is known as Dempster-Shafer Theory. According to this theory some range of probabilities can be used instead of using single number of probabilities. Some mass functions ignore such ambiguities. It is achieved by Bayesian theorem. According to this theory, the posterior probability gets changed. This is done as evidence that helps in getting probability values from the environment required [5]. The difference between the beliefs is used in evidence in the Dempster-Shafer theory.

II. RELATED WORK

Mobile Ad Hoc Networks have been around for long time. They are infrastructure less networks. According to Geetha, in the sloka "yada yada hi dharmasya glanir bhavati bharata abhyuthhanam adharmasya tadatamnan srujamy aham" Krishna says that he would come to this world whenever there is a need for establishment of Dharma. In the same fashion MANET comes in handy when there are emergencies such as hurricanes,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

cyclones, earth quakes, and natural calamities. This is because in emergency situations communications fail and MANET helps in establishing communications again without any fixed infrastructure. MANETs are also widely used in battlefields with trust based security [6]. As it is known in KURUKHSHETHRA, the battle field, a soldier can't manage to come out of PADMAVYUHAA if the route is not known. In the same fashion, in case of MANETs when a packet is corrupted, it can't reach its destination if sufficient security measures lack [6]. In mobile ad hoc networks, maintaining trust of nodes play an important role in ensuring secure communications. The word "trust" refers to the relationship among neighboring nodes in terms of trustworthiness. Trust improves integrity, timeliness and reliability of delivery of messages to next-hop nodes in MANET. The trust also indicates the degree of expectation of mutually benefitted services [7]. When security is a concern it is very important to detect selfish and malicious nodes in network [8]. In MANETs high level of security can be ensured by combining measures such as intrusion and detection and continuous authentication [9]. When MANETs are used in military applications, without security, the nodes are vulnerable to attacks made by adversaries [10]. To provide security trust management is a technique apart from detection of misbehavior in MANETs [10].

Clustering mechanisms also can have impact on the energy usage and network security. In [11] hexagonal clustering is proposed. According to that the WSN is made up of hexagonal clusters. Each hexagon shaped cluster, a cluster head is located. This paper advocates that the sub division of cluster can save the energy consumption. The more it is sub divided, the more it can reduce power consumption. The radius such as R/2, R/3 and R/4 sub divisions save energy worth 50%, 67% and 75% respectively. Trust also can be used with WSN for energy efficiency. In [12] TRACE is proposed which is a centralized Competence and Trust based Energy – efficient routing scheme. This scheme protects WSNs from different kinds of security threats. By helping routing protocol TRACE helps in improving security. The sink or BS in such WSN is more knowledgeable and powerful which involves in maintenance of reliability and trust. It also saves energy significantly. Another aspect to achieve energy efficiency in WSNs is the topology control and routing. The framework proposed in [13] provides energy efficiency in terms of number of hops, transmission, transmission delay and end to end data transmission delay. In [14] yet energy efficient routing protocol is introduced which is end – to –end localized routing that also ensures guaranteed delivery of packets.

Throughput is another important aspect to be considered in MANETs. Efficient node discovery before data transmission helps in finding path of a dislocated node also thus making it efficient. This increases throughput while consumes more energy [15]. In order to transmit data efficiently BER (Bit Error Rate) plays an important role as this can affect possible throughput and also causes delay in transmission. In [16] BER problem is explored and the solution reduced BER and improves throughput. Energy efficient clustering techniques are used to have better resource allocation and improve the lifetime of network [17]. In [18] a framework is proposed to achieve maximum throughput while utilizing less energy. As power consumption is increased its data throughput also increased. WSN clustering also reduced power consumption. In [19] a transmission – power based algorithm is proposed for saving energy. In MANETs trust plays an important role and it can increase security and also energy efficient data transmission. However, it is challenging to achieve it. In [20] the proposed method aimed at achieving reliability, reconfigurability, scalability and availability. It considers social, cognitive and communication networks while taking resource constraints in the given network. The trust management implemented in this paper provides energy efficiency and that also indirectly leads to good security mechanisms in MANET.

In case of trust management the nodes in the network and central authority should have less dependency for trust management in ad hoc networks. It makes it very difficult to compute trust of a node from different levels in the network [6]. Secure Routing Protocol is used in MANETs that can detect and prevent internal attacks. In this context the messages used in route discovery are protected using pair wise secret keys and cryptographic techniques [21]. Trust management that leads to energy efficiency and security is proposed by A. Pirzada & C. McDonald [22] that does not make use of central authority. In pure ad hoc networks, establishing trust based security is explored by [23] by using authentication and confidentiality. The proposed system in this paper combines the concept of trust management and also creating hexagonal clusters to ensure that energy-efficient routing takes place in MANET and also communications are secure.

III. PROPOSED SYSTEM ARCHITECTURE

The proposed system is a new trust based algorithm that ensures detection of colluding nodes and defending the internal attacks made by colluding nodes. The proposed approach is cluster oriented in nature that provides security to MANET. Clustering is involved in the architecture of the proposed system that enables trust computation, route detection and forward node selection process.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

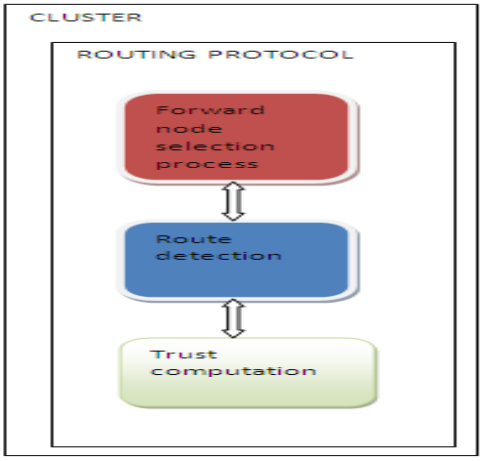


Fig. 1 – Block diagram of proposed system

As can be seen in fig. 1, a cluster has a routing protocol that in turn has operations like forward node selection process, route selection and trust computation. Route detection component is responsible to choose a route that optimizes communication mechanism. The trust computation is responsible to calculate trust that is central to the proposed application to ensure security.

A.Cluster Formation

The aim of proposed application is to minimize transmission delay, energy consumption, and increase overall throughput of the network [1]. Apart from this the proposed mechanism facilitates the detection of colluding nodes and prevention of internal attacks from such nodes. Broadcasting is used in cluster approach for communication. The MANET described here is a collection independent nodes that are mobile in nature and thus the whole network strives to save the bandwidth and other resources [2]. The cluster formation procedure is shown graphically in fig. 2.

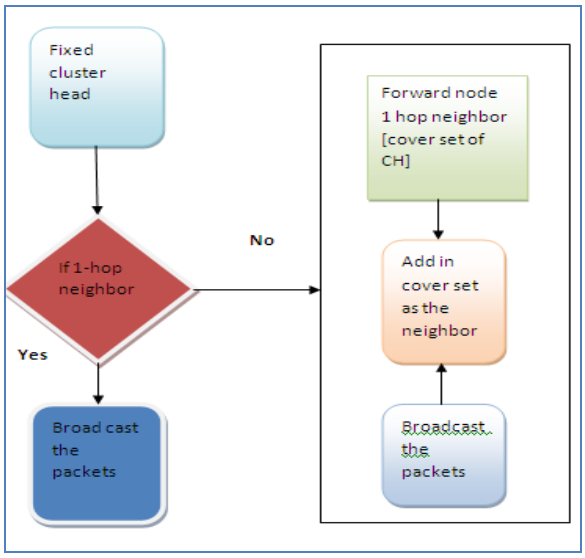


Fig. 2 – Procedure for cluster formation

B.How to avoid broadcast storm problem

Through the forward nodes, as illustrated in fig. 2, acknowledgements of power set is sent to the cluster head. However, cluster head's own covered nodes discard packets when there is no destination ID. While receiving information about piggyback, each and every forward node can confirm that its neighbor set received packet already. Cluster forming is visualized in fig. 2 that is efficient as it can avoid broadcast storm besides making the clusters consuming less resources. The tasks such as route detection, forward node selection and trust computation are fundamentally dependent on cluster formation procedure. The hexagonal cluster formation further reduces the energy requirements by the nodes. With the introduction of hexagonal clustering, the whole MANET becomes energy efficient as the hexagonal structure of clusters involve in communication where the distance between nodes and cluster head is less thus reducing the energy required for communication.

C.Computing Trust

There are two models that can be used to compute trust. They are Baysian Method and Eigen Method. In order to evaluate local nodes, the Baysian model identifies neighbors and collects reputation. Calculating local trust value is done by this method. Therefore its data retrieval is easier and it needs less storage [5]. The Eigen method is used to compute the normalized local trust and then perform aggregation to obtain global trust values. This will help in reducing inauthentic nodes in the MANET. This kind of trust is known as Eigen Trust. Using Eigen method trust value is computed as: $C_{ij} = [(Sum_{ij},0) / \sum_j = max (Sum_{ij},0)]$ Dempster Rule of Combination can be used to overcome the drawbacks of Eigen method. It ignores conflicting evidence by normalizing multiple sources [16]. Using this approach the trust value can be computed as $T(N1) = W_{DP}(N1) \text{ X } T_{DP}(N1) + W_{CP}(N1) \text{ X } T_{CP}(N1)$

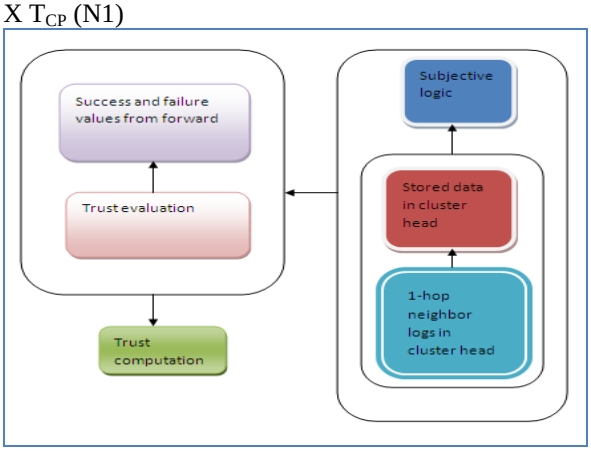


Fig. 3 – Procedure for Trust Management

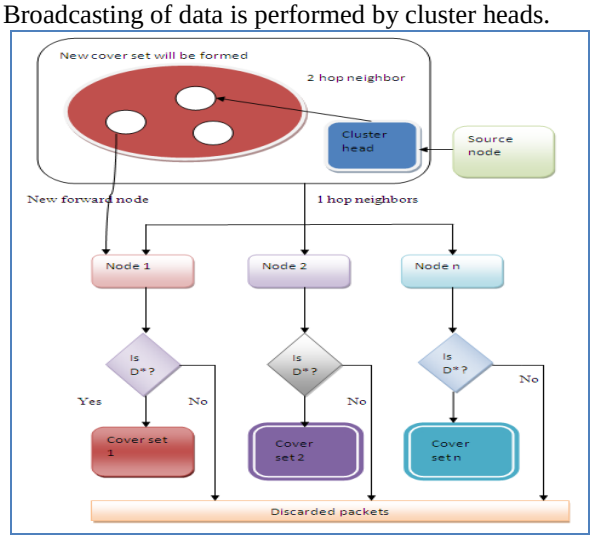
ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

As can be seen in fig. 3, when Dempster-Shafer's combination rule is used the computation of success and failure of every node is done and the trust values are stored in cluster head. In order to determine the trustworthiness of node normalized value is used. The value of N might be positive or negative as per the combination rule. When a node comes back to a cluster after moving to other cluster its trust is considered global trust that can be obtained from the previous cluster head.

D.Forward Node Selection

A node which is one hop neighbor of cluster head is known as forward node. For routing purposes within clusters the forward nodes are used. In order to route between the clusters Gateway nodes are used [7]. Broadcasting of data is performed by cluster heads.



D*=Destination

Fig. 4 – Forward node procedure selection

As can be seen in fig. 4, as soon as a cluster head receives a packet, it forwards to one hop forward node after observing destination. Every forward node has two things known as cover set and neighbor set. One hop neighbors are known as cover sets while other forward nodes are known as neighbor set. When a node transmits a packet, first of all cluster receives packet and then the packet is broadcasted to forward nodes. The path is discarded when the destination id is not found in the cover set of a forward node. The routing information is retrieved by neighbor set and forward set from the cluster head and forwarding nodes.

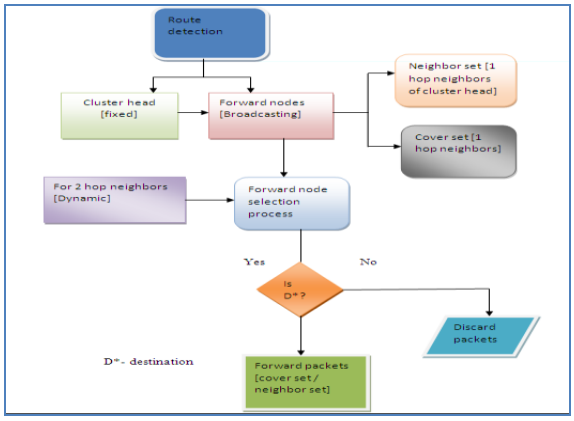


Fig. 5 – Route detection procedure

As can be seen in fig. 5, the route detection is one of the important tasks that are somehow related with trust value computation, energy efficiency and also the clustering mechanism.. The forwarding nodes and cluster head are involved in computation of trust. However, the approach following for hexagonal cluster formation results in energy efficient way of activities such as route discovery, trust management and other communications involved.

IV. RESULTS AND DISCUSSION

This section presents comparison of results among the ADOV, RTSR and the proposed. The environment used for simulation is NS2. The simulation results including end to end delay, packet delivery and throughput are presented in table 1 and used to analyze the proposed algorithm with AODV and RTSR.

Time (ms)	Throughput			Packet Delivery Ratio			End-to-End-Delay		
	aodv	rtsr	P*	aodv	rtsr	P*	aodv	rtsr	P*
10	56	62	64	0.2	0.2	0.18	0	0	0.7
20	102	112	116	0.4	0.5	0.46	15	14	16.2
30	170	182	186	0.6	0.6	0.65	21	24	25.7
40	152	156	167	0.8	0.8	0.93	58	46	43.4
50	248	220	259	1	1.2	1.48	98	78	873.2
60	268	296	315	1.2	1.6	1.8	105	85	79.1
70	251	368	383	1.4	1.7	1.9	111	92	85.4
80	327	405	421	1.6	1.9	2.15	120	98	87.3

P*=Proposed

Table 1 – Values of Performance Metrics

Metrics Used for Simulation Most commonly used parameters in MANETs are end to end delay, throughput, and packet delivery ratio. The time taken to send a packet across the network is known as end to end delay. The amount to data that is successfully transferred from one end to another end is known as throughput. The ratio between the packets sent by the source node and the packets received by destination node successfully is known as packet delivery ratio. The proposed algorithm for route detection process in MANETs.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

```
1     FN broadcasts to its respective CS
2     IF (found DN's ID in CS) {
3     Broadcast to the respective node }
4     ELSE {
5     Don't  broadcast to the NS and Self discard the
      packet
6     }
7     }
8     IF (multi hop nodes) {
9     // refer Fig. 5
10    }
11    DO {
12    Trust will be calculated
13    }WHILE (DN is trusted or not){
14    Using FN's success and failure rates
15    }
16    IF (node is trusted) {
17    Forward the packets
18    }
19    ELSE {
20    Discard the packets
```

Fig. 6 – Algorithm for route detection

V. ANALYSIS

Based on the values provided in table1, RTSR, AODV and proposed are plotted for comparing end to end delay, throughput and packet delivery ratio. Fig. 7 shows the throughput results of proposed method along with RTSR and AODV.

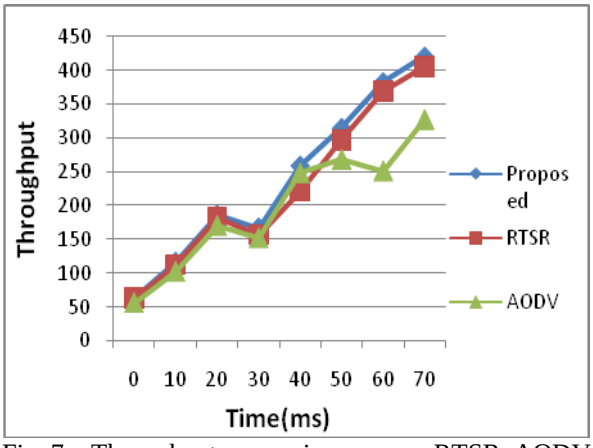


Fig. 7 – Throughput comparison among RTSR, AODV and Proposed As can be seen in fig. 7, it is evident that the proposed method has achieved higher throughput for the reason that its bandwidth and power consumption are less. It also overcomes the overhead caused by acknowledgements by piggybacking a bit during broadcasting.

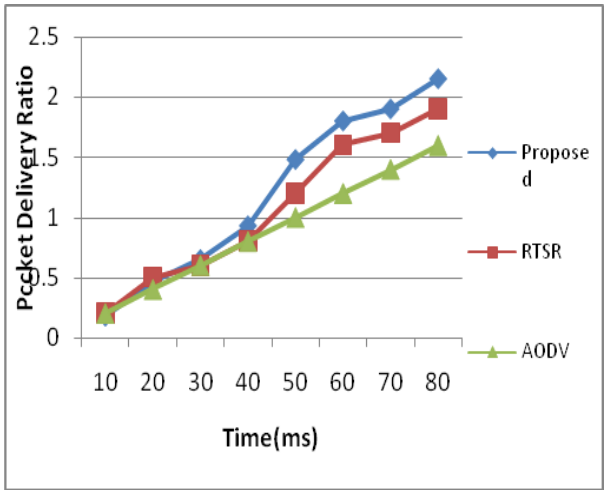


Fig. 8 – Packet delivery ratio among RTSR, AODV and Proposed

In this paper, we studies as the hexagonal cluster structure gives the less energy consumption than regional clustering. Simulation results show that our algorithm is trust and energy efficient accurate with a small communication overhead. This cluster based proposed protocol gives more result than AODV and RTSR. Whenever number of delivery packets are more end to end delivery is less as can be seen in fig. 8, it is evident that packet delivery ratio of proposed method is more when compared with AODV and RTSR. The reason behind this is that it makes use of trust management technique, consumes less bandwidth for the operations in presence of colluding nodes and also energy efficient, it is evident that the end to end delay of the proposed approach is decreased

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

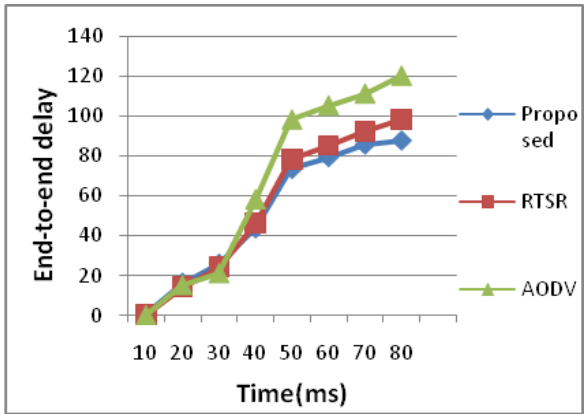


Fig. 9 – End – to – End Delay Analysis Among RTSR, AODV and Proposed

This is because proper retrieval of route discovery information using trusts and energy efficient hexagonal clustering.

VI. CONCLUSION

Security mechanism and power efficiency is important in order to ensure secure communication between end to end users in mobile ad hoc networks. Discarding of the path is main object when the destination id is not found as the energy consumption as a whole. compared to AODV and RTSR. Even though at less power rating this proposed protocol gives more throughput than existing protocols. There is an issue of cochannel interference in hexagonal clustering. There will be a need of decrease cochannel interference which happens to reduce energy consumption. This issue will be explored in our future research.

REFERENCES

[1] S.Neelavathy Pari, B.Narmadhadevi, and Sridharan Duraisamy. "Requisite Trust-Based Secure Routing Protocol for MANETs",ICRTIT pp276-281., IEEE 2012.

[2]. J. Broth, D.A. Maltz , D . B. Johnson, Y.C. H u, and J. Jetcheva."A performance comparison of multi hop ad–hoc network routing protocols" *in Proc., MOBICOM' 98,1998*, pp. 85-97.

[3]. X. Li, M.R. Lyu & J. Liu, "A trust model based routing protocol for secure ad hoc networks" in Proc., *IEEE aerospace conference* , vol. 2, pp. 1286–1295, March 2004.

[4]. Dempster's rule of combination , Expert systems/Dempster-shafer theory, http://en.wikibooks.org/wiki/Expert_Systems/Dempster-Shafer_Theory.

[5]. Kari Sentz,"Combination of Evidence in Dempster-Shafer Theory", *Computer and Information Science journal* ,vol. 853, pp.37- 72, 2002.

[6].A.A. Pirzada, C. McDonald, Trust establishment in pure ad-hoc networks, in: 1465 Wireless Personal Communications, vol. 37, pp. 139–168, 2006.

[7]. Hui Xia a Q1 , Zhiping Jia a,Lei Ju a, Xin Li a, Edwin H.-M. Sha " Impact of trust model on on-demand multi-path routing in mobile ad hoc networks", *Computer Communications*, 2012 Elsevier.

[8]. Koul, A.; Patel, R.B.; Bhat, V.K.; , "A system level security for Mobile Ad hoc Networks," Computer Research and Development (ICCRD), 2011 3rd International Conference on , vol.3, no., pp.72-76, 11-13 March 2011 .

[9]. Thomas M. Chen and Varadharajan Venkataramanan ,Southern Methodist University, "Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks" In IEEE Internet Computing Published by the IEEE Computer Society November December 2005.

[10]. Wenjia Li, James Parker , Anupam Joshi " Security Through Collaboration and Trust in MANETs" Springer Link , vol. 17,issue 3, pages. 342-352, June. 2012.

[11]. Dajin Wang; Li Xu; Jing Peng; Robila, S.; , "Subdividing Hexagon-Clustered Wireless Sensor Networks for Power-Efficiency," Communications and Mobile Computing, 2009. CMC '09. WRI International Conference on , vol.2, no., pp.454-458, 6-8 Jan. 2009

[12]. Tajeddine, A.; Kayssi, A.; Chehab, A.; , "TRACE: A centralized Trust And Competence-based Energy-efficient routing scheme for wireless sensor networks," Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International , vol., no., pp.953-958, 4-8 July 2011.

[13]. Lutful Karim1*, Tarek El Salti1, Nidal Nasser2 and Qusay H Mahmoud1 "The significant impact of a set of topologies on wireless sensor networks, EURASIP Journal on Wireless Communications and Networking 2012.

[14]. Essia Hamouda, Nathalie Mitton, Bogdan Pavkovic,David Simplot-Ryl, " Energy-aware Georouting with Guaranteed Delivery in Wireless Sensor Networks with Obstacles" International Journal of Wireless Information Networks, September 2009, Volume 16, Issue 3, pp 142-153.

[15]. Ramchand V and D.K. Lobiyal ,"Throughput Analysis of Power Control BMAC Protocol in WSN" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 3, June 2012.

[16]. M.R.Ebenezar jebarani1and T.Jayanthy ,"An Analysis of Various Parameters in Wireless Sensor Networks using Adaptive FEC Technique" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.3, September 2010.

[17]. Guan Xin; Wang YongXin; Liu Fang; , "An Energy-Efficient Clustering Technique for Wireless Sensor Networks," Networking, Architecture, and Storage, 2008. NAS '08. International Conference on , vol., no., pp.248-252, 12-14 June 2008.

[18]. Xun Chen; Chin Choy Chai; Yong Huat Chew; , "Constrained power allocation algorithm for rate adaptive MIMO system," Spread Spectrum Techniques and Applications, 2004 IEEE Eighth International Symposium on , vol., no., pp. 924- 928, 30 Aug -2 Sept. 2004.

[19]. Parikha Chawla, Parmender Singh, Taruna Sikka ,"Enhance Throughput in Wireless Sensor Network Using Topology Control Approach", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[20]. Jin-Hee Cho; Swami, A.; Ing-Ray Chen; , "A Survey on Trust Management for Mobile Ad Hoc Networks," Communications Surveys & Tutorials, IEEE , vol.13, no.4,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

[21]. Ming Yu; Mengchu Zhou; Wei Su; , "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments," Vehicular Technology, IEEE Transactions on , vol.58, no.1, pp.449-460, Jan. 2009.
[22]. A. Pirzada & C. McDonald, "Establishing trust in pure ad-hoc networks", in Proceedingsof the 27th Australian conference on computer science(ACSC'04) 2004 , vol. 26, pp. 41-46.
[23]. Renu Mishra, Inderpreet Kaur & Sanjeev sharma, "New trust based security method for mobile ad-hoc networks", in Proc., International Journal of Compter Science snd Security, vol. 4, pp. 346-351, 2010.
[24]. Haidar Safa , Hassan Artail & Diana Tabet ,"A cluster-based trustaware routing protocol for mobile ad hoc networks", Springer Link , vol.16, pp. 969-984, May. 2010.
[25].H. Lim and C. Kim, "Flooding in wireless ad hoc networks", *Computer Communications Journal*, vol.24, no.3-4, pp. 353- 363, 2001.

Biography

Prof.P.PADMANABHAM (M.Tech (AE), M.Tech(CS), Ph.D(CS)-FIETE) Double Post-Graduate in Engineering & Technology (M.Tech-Computer Science and M.Tech-Advanced Electronics) and Ph.D in Computer Science & Engineering. Over 40 years of experience in Technical Education in the areas of Teaching, Administration, Research and Consultancy. Currently working as Professor of Computer Science & Engineering and Director (Academics) Bharat Institute of Engineering and Technology since August 2005. He worked as a Professor of CSE & Director I/C – School of Information Technology, Jawaharlal Nehru Technological University, Hyderabad(July 2004 to Aug 2005). He won the prestigious "Best Teacher" award of Indian Society for Technical Education (ISTE) in the year 1990. Currently Guiding Ten Ph.D students and One M.S Student. He authored three books in the discipline of Computer Science and Engineering and the fourth is in press for publication.

Dr. BHIMA PRABHAKARA RAO Professor of ECE, Dept of Electronics & Communication Engg,University College of Engineering,Kakinada,JNTU Campus. Over 27 Years of teaching and 19 Years of Research and Development experience. He has membership of Professional Bodies of FIE, FIETE, MISTE, and MIEEE. His field of specialization in Signal Processing & Communications. Presently 12 students are doing their Ph.D under his extreme guidance. Three Scholars were awarded Ph.D with his guidance. He published more than 75 publications in national and international journals. He successfully completed two AICTE Projects. He published two books on Networks, Signals & systems for JNTU, Hyderabad.

Vemana Chary is pursuing PhD from JNTUK, Kakinada, Andhra Pradesh in Mobile Communications. He has guided many students under projects having an experience of 13 years in academic under teaching. He is currently working as an Associate Professor in the ECE Department at Bharat Institute of Engineering & Technology, Hyderabad..His areas of research interest includes Wireless and Mobile communications, Digital signal and image processing, Network Security Network Management, QoS, Policy-Based Network.