Trust Based Bayesian Inference and Dempster-Shafer Theory to Achieve Security in MANET

Bhumika Shah[1], Juhi Kaneria[2]

[1]Student, Information Technology, Parul Institute of Engineering & Technology, Gujrate,India

[2] Assistant. Professor, Computer Science and Engineering, Parul Institute of Engineering & Technology, Gujrate,India

ABSTRACT

MANET consist of many small devices communicating spontaneously over the air (wireless).The topology of the network is changing frequently because of the mobile nature of its nodes. Ad hoc finally induces that there are no such things as fixed routers, therefore every node has to act as a router for its neighbors. Trust-based schemes are considered as effective mechanisms associated with cryptographic techniques for thwarting a variety of attacks. Because of the properties of MANET, trust establishment needs an intelligent approach to identify attackers' misbehavior. A routing protocol for MANET should give incentives for acting correctly and it should be able to detect misbehaving nodes and punish them. In MANET no priori trust relationships and no central trustworthy authorities exist. The goal is to establish trust relationships by using a reputation-based trust management scheme. This can be done by getting reputation for a node and combining this with personal observations about its behavior. Bayesian interface is used for direct observation and Dempster-Shafer theory is used to calculate trust value based on indirect observation.

Keyword: - *Trust ,Reputation***,** *Dempster-Shafer theory, Bayesian interface.*

1. INTRODUCTION

MANETs are a kind of temporal and self-organized networks, that are unit appropriate for military science environments and disaster recovery situations. as a result of its characteristics, e.g., no needs of infrastructure, MANETs are attracting plenty of attention. during this sort of networks, nodes will type a distributed network and communicate with one another via wireless medium. Every node has join forces with different nodes so as to deliver traffic from supply nodes to destination nodes. Security being the prime concern to supply protected communication between mobile nodes in a very hostile surroundings. As compared to wireline networks, the distinctive property of mobile impromptu networks cause variety of nontrivial challenges to security way, like open peer-to-peer spec, shared wireless medium, strict resource constraints, and extremely dynamic constellation. These problems clearly build a situation for building multifence security solutions that deliver the goods each broad protection and fascinating network performance.

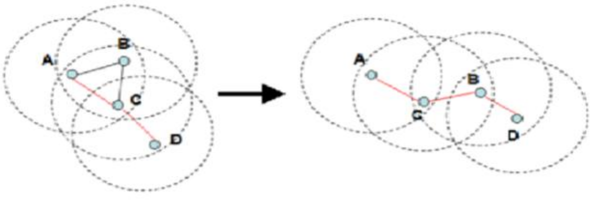

Fig 1- Example of a simple network with four participating nodes [5]

1.1 Problem Statement

- Our motive is to design a secure routing protocol without introducing huge overhead or destroying the self-organization nature of MANET.
- Trust calculation of the nodes dosnt consume much time.
- No need to sign and verify digital signature at every routing message.

1.2 Motivation

The main motivation of this project has emerged with the deliberate amount of work still in detecting the malicious and selfish node in MANET. Selfishness that causes lack of node activity cannot be solved by classical security means that aim at verifying the correctness and integrity of an operation.

Misbehaviour of nodes network operations (routing, packet forwarding) could vary from easy stinginess or lack of collaboration as a result of the necessity for power saving to active attacks.

Selfish nodes use the network, saving battery power for own communications: no injury to other nodes. Malicious and selfish nodes aim at damaging different nodes by inflicting network outage by partitioning whereas saving battery life isn't a priority.

Decision making mechanism for different applications are:

- Intrusion detection
- Key management
- Access management
- Authentication

2. Routing Protocols in MANET

This section discuss regarding differing types of protocols employed in mobile spontaneous network. Additionally comparison between completely different routing protocols with relation to specific parameters.

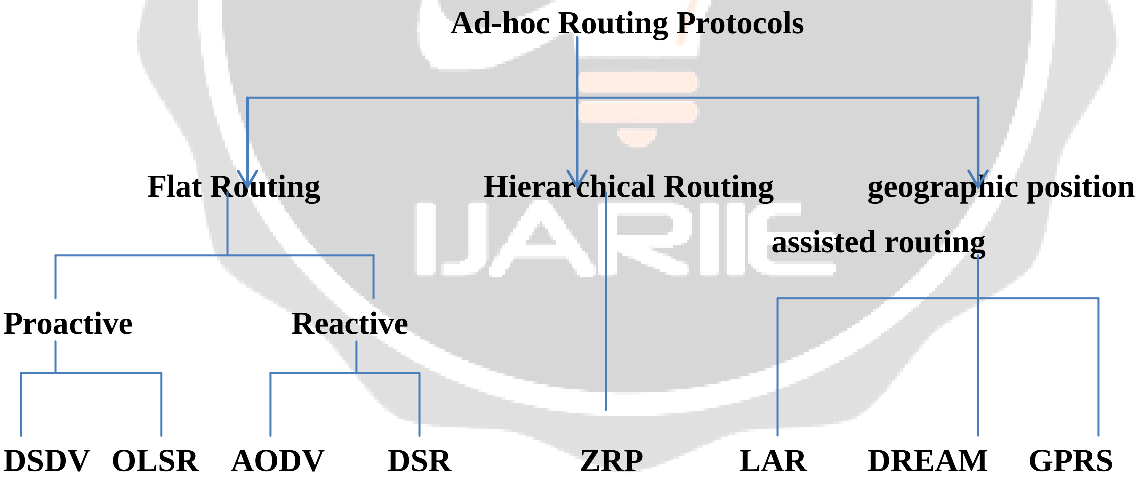

Fig 2: Classification of Routing Protocols MANETs[1]

2.2.1 Ad-hoc On Demand Distance Vector (AODV)

AODV could be a reactive protocol, i.e., that the routes area unit created and maintained only they're required. The routing table stores the knowledge regarding future hop to the destination and a sequence range that is received from the destination and indicating the freshness of the received packets . Additionally the knowledge regarding the active neighbors is received throughout the routing of the destination host.

- Route Request(RREQs)

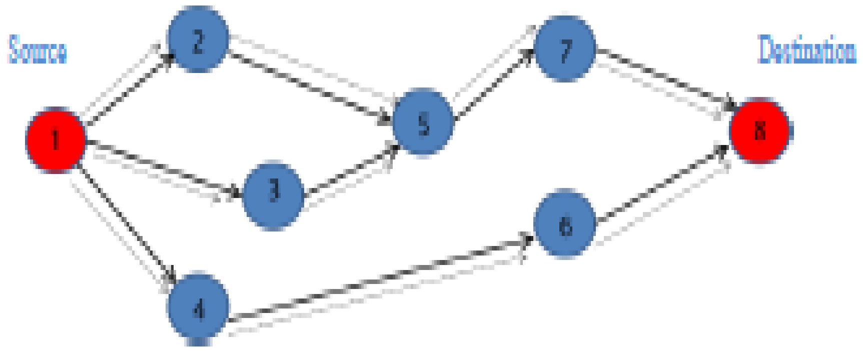

Fig3: Route Request(RREQs) Packets[1]

- Route Replies(RREPs)

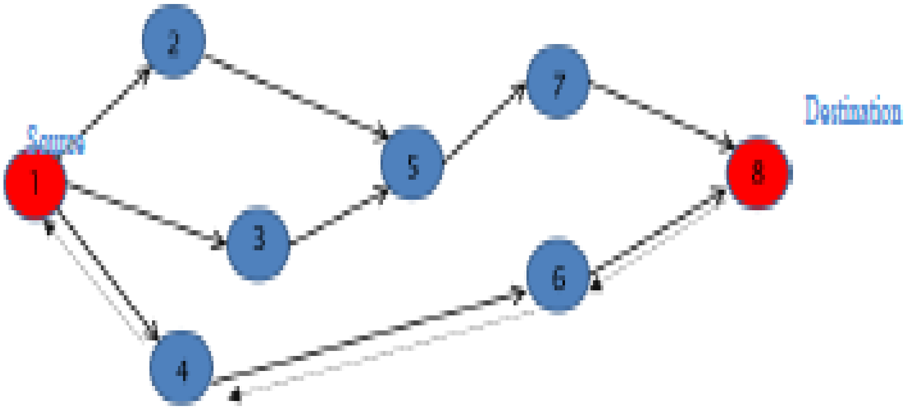

Fig 4: Route Replies(RREPs) Packets[1]

- Route Errors(RERRs)

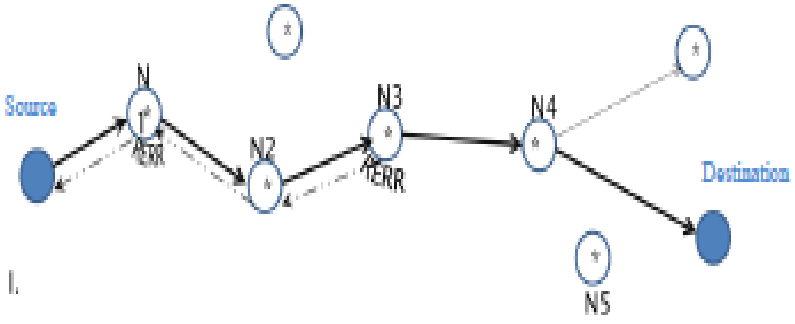

Fig 5: Route Errors (RERRs) Packets[1]

Advantages
1) It is a routing protocol in which doesn't need any central body system to manage the routing method.

2) The overhead of the messages is less.
3) The AODV protocol could be a loop free and avoids the reckoning to infinity drawback, that were typical to the classical distance vector routing protocols, by the usage of the sequence numbers.

2.2.2 Optimized Link State Routing Protocol

Optimized link state routing [10] can be a proactive protocol there in, each node intermittently broadcasts its routing table, allowing each node to make associate comprehensive browse of the network topology. The episodic nature of this protocol creates AN large amount of overhead so on cut back overhead, it limits the number of mobile nodes that will forward network wide traffic and for this purpose it use multi purpose relays (MPRs), that unit in command of forwarding routing messages and optimization for flooding operation. Mobile nodes, that unit elect as MPRs can forward management traffic and decrease the dimensions of management messages. MPRs unit chosen by a node, such that, it\'s planning to reach each a pair of hop neighbor via a minimum of 1 MPR, then it\'ll forward packets. quality causes, route modification and topology changes very ofttimes and topology management (TC) messages unit broadcasted throughout the network. All mobile nodes maintain the routing table that contains routes to any or all or any approachable destination nodes.
Advantages
1) The reactiveness to the topological changes is adjusted by ever-changing the interval for broadcasting the how-do-you-do messages.
2) Due to the OLSR routing protocol simplicity in exploitation interfaces, it's simple to integrate the routing protocol within the existing in operation systems, while not ever-changing the format of the header of the informatics messages.
3) OLSR protocol is compatible for the appliance that doesn't enable the long delays within the transmission of the info packets.

2.2.3 Dynamic supply Routing protocol (DSR)

The dynamic supply routing protocol (DSR) is associate on demand routing protocol. DSR is easy and economical routing protocol designed specifically to be used in multi-hop wireless spontanepous networks of mobile nodes. The DSR protocol consists of 2 main mechanisms that employment togetherto enable the invention and maintenance of supply route within the spontanepous network.

3. Uncertain Reasoning

Most tasks requiring intelligent behavior have a point of uncertainty related to them. the sort of uncertainty that may occur in knowledge-based systems is also caused by issues with the information. For example: knowledge may well be missing or inaccessible,Data may well be gift however unreliable or ambiguous owing to measuring errors.The illustration of the information is also imprecise or inconsistent.
1) knowledge could be user’s best guess.
2) knowledge is also supported defaults and therefore the defaults might have exceptions.
The uncertainty can also be caused by the diagrammatical information since it'd
1.Represent best guesses of the specialists that square measure supported plausible or applied math associations they need determined.
2.Not be acceptable altogether things (e.g., might have indeterminate applicability)
Given these varied sources of errors, most knowledge-based systems need the incorporation of some style of uncertainty management.
Three ways of handling uncertainty:

- Probabilistic reasoning.
- Certainty factors
- Dempster-Shafer Theory

2.3.1 Probabilistic reasoning

Bayes’ Theorem
Conditional probability is defined as

$$P(H \mid E) = \frac{P(H \cap E)}{P(E)}, \text{ for } P(E) \neq 0.$$

i.e., the conditional probability of H given E.

In real-life practice, the probability P(H | E) cannot always be found in the literature or obtained from statistical analysis. The conditional probabilities

$$P(E \mid H)$$

however often are easier to come by;

Thus

$$P(H \mid E) = \frac{P(E \mid H)\, P(H)}{P(E)}$$

Hypothetical reasoning and backward induction

1) Bayes’ Theorem is commonly used for decision tree analysis of business and the social sciences.

2) The method of Bayesian decision making is also used in expert system PROSPECTOR.

2.3.2Bayesian inference

Is a method of statistical inference in which Bayes' rule is used to update the probability estimate for a hypothesis as additional evidence is acquired. Bayesian updating is an important technique throughout statistics, and especially in mathematical statistics. For some cases, exhibiting a Bayesian derivation for a statistical method automatically ensures that the method works as well as any competing method. Bayesian updating is especially important in the dynamic analysis of a sequence of data. Bayesian inference has found application in a range of fields including science, engineering, philosophy, medicine and law.

In the philosophy of decision theory, Bayesian inference is closely related to discussions of subjective probability, often called "Bayesian probability". Bayesian probability provides a rational method for updating beliefs

Bayesian inference derives the posterior probability as a consequence of two antecedents, a prior probability and a "likelihood function" derived from a probability model for the data to be observed. Bayesian inference computes the posterior probability according to Bayes' rule:

$$P(H \mid E) = \frac{P(E \mid H)\, P(H)}{P(E)}$$

Where

- denotes a conditional probability; more specifically, it means given.
- H stands for any hypothesis whose probability may be affected by data (called evidence below). Often there are competing hypotheses, from which one chooses the most probable.
- the evidence E corresponds to new data that were not used in computing the prior probability.
- P(H) the prior probability, is the probability of H before E is observed. This indicates one's previous estimate of the probability that a hypothesis is true, before gaining the current evidence.
- P(H | E) the posterior probability, is the probability of given , i.e., after is observed. This tells us what we want to know: the probability of a hypothesis given the observed evidence.
- P(E | H) is the probability of observing E given H. As a function of with fixed, this is the likelihood. The likelihood function should not be confused with , P(H | E) as a function of H rather than of E. It indicates the compatibility of the evidence with the given hypothesis.
- P(E) is sometimes termed the marginal likelihood or "model evidence". This factor is the same for all possible hypotheses being considered. (This can be seen by the fact that the hypothesis H does not appear anywhere in the symbol, unlike for all the other factors.)

Advantages and disadvantages of Bayesian methods

- The Bayesian methods have a number of advantages that indicates their suitability in uncertainty management. Most significant is their sound theoretical foundation in probability theory. Thus, they are currently the most mature of all of the uncertainty reasoning methods.
- While Bayesian methods are more developed than the other uncertainty methods, they are not without faults.

1.They require a significant amount of probability data to construct a knowledge base. Furthermore, human experts are normally uncertain and uncomfortable about the probabilities they are providing.

2.If they are statistically based, the sample sizes must be sufficient so the probabilities obtained are accurate. If human experts have provided the values, are the values consistent and comprehensive?
3.Often the type of relationship between the hypothesis and evidence is important in determining how the uncertainty will be managed. Reducing these associations to simple numbers removes relevant information that might be needed for successful reasoning about the uncertainties. For example, Bayesian-based medical diagnostic systems have failed to gain acceptance because physicians distrust systems that cannot provide explanations describing how a conclusion was reached (a feature difficult to provide in a Bayesian-based system).
4.The reduction of the associations to numbers also eliminated using this knowledge within other tasks. For example, the associations that would enable the system to explain its reasoning to a user are lost, as is the ability to browse through the hierarchy of evidences to hypotheses.

2.3.3 Dempster-Shafer Theory

Here we discuss another method for handling uncertainty. It is called Dempster-Shafer theory. It is evolved during the 1960s and 1970s through the efforts of Arthur Dempster and one of his students, Glenn Shafer.
1) This theory was designed as a mathematical theory of evidence.
2) The development of the theory has been motivated by the observation that probability theory is not able to distinguish between uncertainty and ignorance owing to incomplete information.

Difficulty with the Dempster-Shafer theory
1) One problem is with standardization and contrary to our expectation.
2) Ignores the assumption about things that doesn't exist.

4.SIMULATION

The implementation result of a Bayesian Interface and Dempster Shafer theory to achieve Trust Based Routing in Mobile Ad-hoc Networks is exhibited. For implementation and result analysis, AODV Protocol is used in Network Simulator.

4.1 Simulation results

Experiments are performed to measure the Packet delivery Ratio, Throughput and End-to-End Delay with calculating the Trust Value of the node depending on the direct observation between the two nodes and reputation from the intermediate nodes.

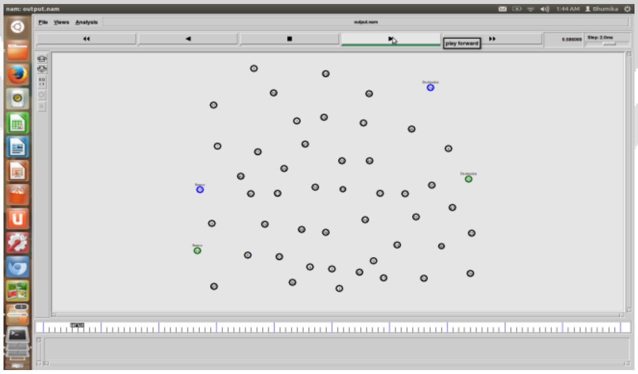

Fig 6: Creating source and Destination nodes

Figure 6 shows the scenario of 50 nodes in network under MANET in which Packets are transmitted using AODV Routing Protocol. Scenario shows the source node 15,19 and destination node 24,28 by using AODV protocol.

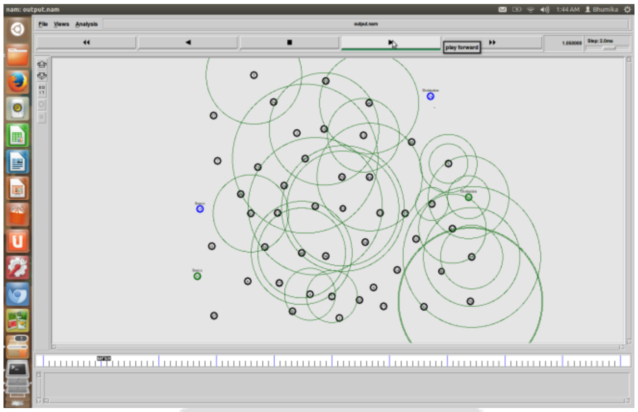

Fig 7 RREQ packet Message Broadcasting

Figure 7 shows the broadcasting of the RREQ packets from source to destination.in the above scenario Node 15 is broadcasting the RREQ packet to all the intermediate nodes in order to reach the destination node 24.

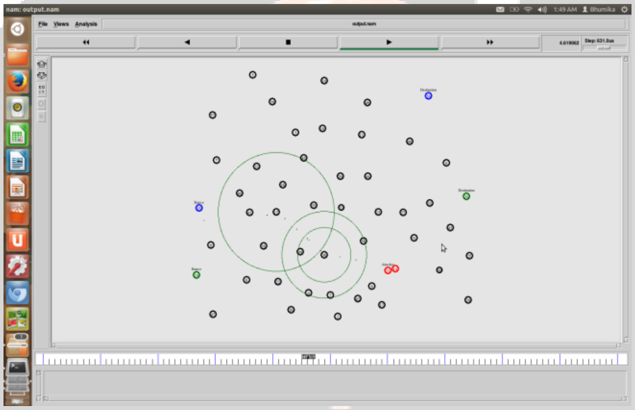

Fig 8 Attacker Node

4.2 Result analysis:

This section shows the result analysis of the different Experimental Parameters. Parameters such as Packet Delivery Ratio. Throughput, End-to-End Delay are considered. Here the PDR is calculated on the basis of no of packets send to the total no of packets for both systems to compare their values. Throughput defines as the total number of packets delivered over the total simulation time. The average end to end delay of knowledge packet is that the interval between the info packet generation time and therefore the time once the last bit arrives at the destination.

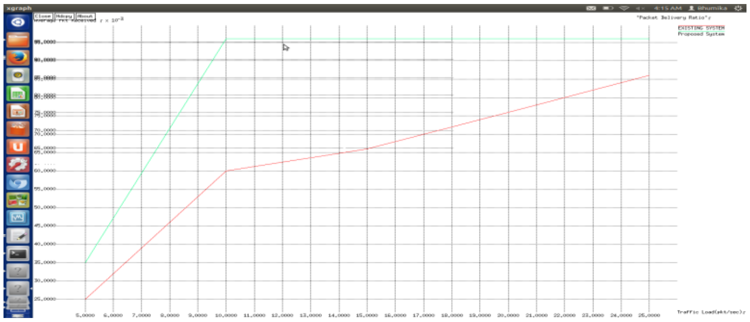

Fig 9 Result of Packet Delivery Ratio

Figure 9 shows the result analysis of the existing and proposed system of the packet ratio delivery.

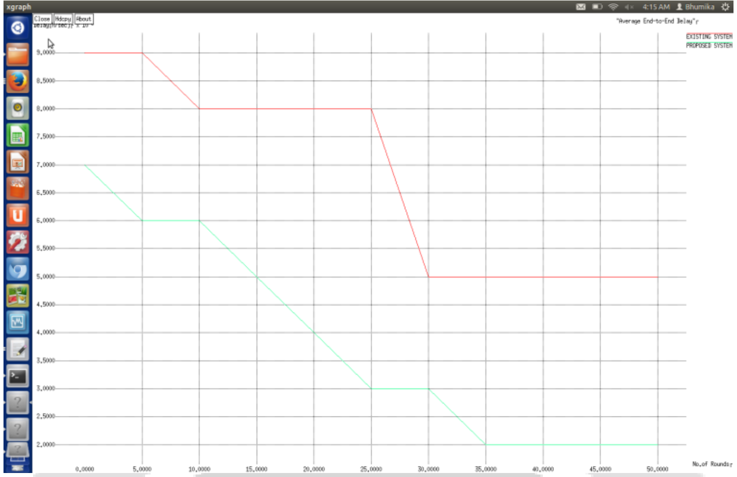

Fig 10 Result of End-to-End Delay

Figure 10 shows the result analysis of the existing and proposed system of the Average End-to-End Delay

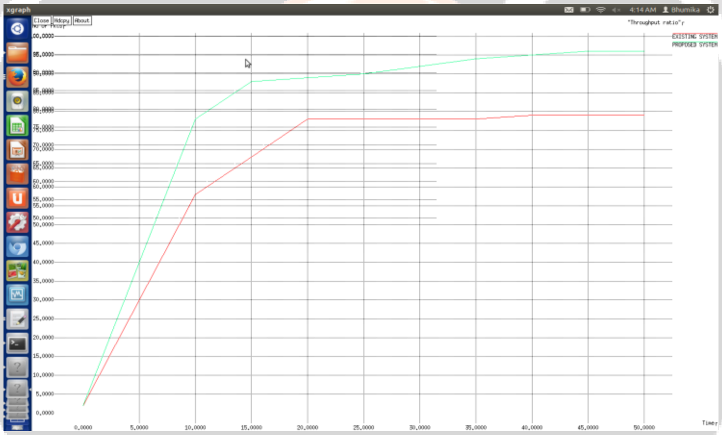

Fig 5.11 Result of Throughput

Figure 11 shows the result analysis of the existing and proposed system of the Average End-to-End Delay.

5. CONCLUSIONS

The proposed algorithm focus on the evaluating the accurate trust value of each node. In the proposed algorithm Trust is evaluated based on direct and indirect observation of the node. The direct observation is evaluated based on Bayesian interface and indirect observation based on Dempster Shafer theory. Combination of these two values in the trust model, is use to obtain more precise trust value of the nodes in MANETs. Also parameters used in the existing system such as Throughput, Average End-to-End Delay will be improved and the other experimental parameters will be added.

REFERENCES

[1]. Y. Wang, F. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1616–1627, 2014.

[2] Z. Wei, H. Tang, F. R. Yu, and M. Wang, "Security enhancement for mobile ad hoc networks routing with OLSRv2," in *Proc. SPIE Defence, Security, and Sensing 2013*, (Baltimore, MD, USA), Apr. 2013.

[3] Q. Guan, F. Yu, S. Jiang, and V. Leung, "Joint topology control and security in mobile ad hoc networks with cooperative communications," *IEEE Trans. Veh. Tech.*, vol. 61, no. 6, pp. 2674–2685, 2012.

[4] J. Loo, J. Lloret, and J. H. Ortiz, Mobile Ad Hoc Networks:Current Status and Future Trends. CRC Press, 2011.

[5] B. Elizabeth, R. Aaishwarya, P. Kiruthika, M. Shrada, A. Prakash, and V.Uthariaraj, "Bayesian based confidence model for trust inference in manets," in *Proc. IEEE ICRTIT'11*, (Chennai, Tamil Nadu, India), Jun. 2011.

[6] J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

[7] Han Yu, Zhiqi Shen, Chunyan Miao, Cyril Leung, and Dusit Niyato,"A Survey of Trust and Reputation Management System in Wireless Communications," proc. of the IEEE, 2010.

[8] Pedro B. Velloso, Rafael P Laufer, Daniel de O. Cunha, Otto Carlos M.B. Duarte, and Guy Pujolle." Trust Management In Mobile Ad hoc Networks Using a Scalable Maturity Based Model, IEEE transactions on networks and Service Management Vol. & No. 3 Sept. 2010. pp172 - 185.

[9] A. Darwiche, *Modeling and reasoning with Bayesian Networks.* Cambridge University Press, 2009.

[10] M. Momani, S. Challa, and R. Alhmouz, "BNWSN: Bayesian network trust model for wireless sensor networks," in *Proc. MIC-CCA 2008*, (Amman), Aug. 2008.