Survey paper on Evaluating Trust and Reputation Using Uncertain Reasoning in MANET

Bhumika R. Shah[1], Juhi Kaneria[2]
[1]Student, I.T Department, Gujarat Technical University, PIET, India
[2]Professor, CSE Department, Gujarat Technical University, PIET, India

Abstract

Towards wide-spread activity, security issues become a central concern. Whereas plenty of research has targeted on making these networks doable and useful, security has received little or no attention. we've got a bent to gift a collection of security protocols optimized for Mobile impromptu Networks: victimization Trust and name metric along with unsure reasoning. unsure Reasoning includes two quite observation: Direct observation and Indirect observation. to boost positive parameters like Packet Delivery relation, Throughput, Overhead and finish to finish Delay.

Keywords: — *Trust, Reputation, Uncertain Reasoning, Packet Delivery quantitative relation, Throughput, Overhead and finish to finish Delay*

1.Introduction

MANETs square measure a sort of temporal and self-organized networks, that square measure applicable for field of study environments and disaster recovery things. as a result of its distinctive characteristics, e.g., no wants of infrastructure, MANETs square measure attracting many attention. throughout this form of networks, nodes can blood type distributed network as well as communicate with each other via wireless medium. each node has to affix forces with totally different nodes thus on deliver traffic from provide nodes to destination nodes. Security has become a primary concern thus on turn out protected communication between mobile nodes throughout a hostile surroundings. not just like the wireline networks, the distinctive characteristics of mobile unplanned networks cause form of nontrivial challenges to security vogue, like open peer-to-peer specification, shared wireless medium, tight resource constraints, and very dynamic constellation. These challenges clearly produce a case for building multifence security solutions that win every broad protection and engaging network performance.

A mobile unplanned network (MANET) is Associate in Nursing autonomous system of mobile hosts (MHs) that transmit data across a wireless communication medium. MHs act as routers collectively. thus the functioning of Manet depends on the trust [1] and cooperation among nodes. trustworthy MHs ar selected for routing as a results of it will guarantee successful routing whereas not inflicting any injury to the data to be routed. trustworthy routing collectively identifies region node and avoids it so as that packet is not forwarded through it otherwise packets might even be born. together with this, resource utilization of mobile hosts in routing is to boot taken into thought.

Traditional security mechanisms will usually defend resources from malicious users, by proscribing access to exclusively approved users. However, information suppliers can as an example act deceitfully by providing false or dishonest information, and ancient security mechanisms ar unable to protect against form of threat. Trust and name systems on the other hand can offer protection against such threats.

1.1 kinds of Security Attacks

1)Routing loop attacks: A malicious node might modify routing packets in such however that packets traverse a cycle thus do not reach the supposed destination .

2) hollow attacks: a group of cooperating spiteful nodes can pretend to join 2 distant points at intervals the network connection among a low-latency communication between two link remarked as a hollow link, inflicting disruptions in ancient traffic load and flow.

3) Blackhole attacks: A malicious node, the so remarked as half node, might forever respond fully to route requests even once it does not have correct routing information. The half can drop all packets forwarded to it.

4) Grayhole attacks: A malicious node might selectively drop packets.For example, the malicious node might forward routing packets but not data packets. Similarly, a depression bad person attracts nodes to route through it thus selectively routes packets.

5) DoS attacks: A malicious node might block the standard use or management of communications facilities, as AN example, by inflicting excessive resource consumption.

6) False information otherwise false recommendation: A mischievous node might conspire and provide false recommendations/information to isolate sensible nodes whereas keeping malicious nodes connected. at intervals the stacking attack, a malicious node keeps grumbling many peer node and creates the peer's negative name.

7) Incomplete info: A malicious node won't collaborate in providing correct or complete data. usually compromised nodes conspire to perform this attack. However, node quality or link failure, prevailing in painter.

8) Packet modification/insertion: A malicious node might modify packets or insert malicious packets like packets with incorrect routing information.

9) Newcomer attacks: A malicious node might discard its dangerous name or distrust by registering as a replacement user. The malicious node just leaves the system and joins all over again for trust revocation, flushing out its previous dangerous history and obtaining right down to accumulate new trust.

10) Sybil attacks: A malicious node can use multiple network identities which could have an impression on topology maintenance and fault tolerant schemes like multi-path routing.

11) Blackmailing: A mischievous node can blackmail a different node by spreading false information that an additional node is malicious otherwise misbehaving. this could generate important amount of traffic and ultimately disrupt the usefulness of the whole network. This attack square measure usually seen as false accusation and DoS attacks at intervals the sense that false information is disseminated leading to a significant amount of resource consumption.

12) Replay attacks: A malicious node might replay earlier transmitted packets. If the packets embody data, this might not cause trouble, and conjointly the receiving node merely discards incorrect packets. However, if the resister replays route requests, routing table information would become incorrect, and up to date locations and routing information might build nodes unapproachable.

13) Selective misbehaving attacks: A malicious node behaves badly but selectively to various nodes.

14) On-off attacks: A malicious node might instead behave well and badly to stay unobserved whereas disrupting services.

15) Conflicting behaviour attacks: A malicious node might behave otherwise to nodes in many groups to make the opinions from the assorted sensible groups conflicting, and ultimately end in non-trusted relationships.

1.2 Routing Protocols in painter

This section discuss relating to different types of protocols utilized in mobile unintentional network. collectively comparison between fully totally different routing protocols with connectedness specific parameters.

1.2.1 impromptu On Demand Distance Vector (AODV)

AODV could also be a reactive protocol, i.e., thus the routes area unit created and maintained on condition that they are needed. The routing table stores the information relating to following hop to the destination and a sequence selection that's received from the destination and indicating the freshness of the received packets . collectively the information relating to the active neighbours is received throughout the routing of the destination host.

Advantages

1)Because the AODV protocol could also be a flat routing protocol it does not wish any centrosome system to handle the routing technique.

2) The overhead of the messages little. If host has the route information at intervals the Routing Table relating to active routes at intervals the network, then the overhead of the routing technique square measure getting to be minimal[16].

3) The AODV protocol could also be a loop free and avoids the count to infinity disadvantage, that were typical to the classical distance vector routing protocols, by the usage of the sequence numbers.

1.2.2 Optimized Link State Routing Protocol

Optimized link state routing [10] could also be a proactive protocol in this, every node intermittently broadcasts details through routing table, allowing every node to make associate inclusive check of the network topology with different techniques. The episodic character of this protocol creates AN oversized amount of overhead along with then on cut back overhead, it confines the number of mobile nodes which is capable to forward network huge traffic along with for this reason it use multipurpose relays (MPRs), that area unit declarable for forwarding routing messages as well as optimization for flooding operation. Mobile nodes, that area unit selected as MPRs can forward management traffic and decrease the size of management messages. MPRs area unit chosen by a node, such that, it ought to reach each two hop neighbor via a minimum of 1 MPR, then it'll forward packets.Mobility causes, route modification and topology changes really usually and topology management (TC) messages area component broadcasted throughout the set of connection network. Every one mobile devices node maintains the routing table that includes routes to all otherwise accessible destination nodes.

Advantages

1) OLSR is to boot a flat routing protocol, it does not wish centrosome system to handle its routing technique. The proactive characteristic of the protocol provides that the protocol has all the routing information to all or any or any participated hosts at intervals the network.

2) The reactiveness to the topological changes is adjusted by propelling the number for broadcasting the howdy messages.

3) as a result of the OLSR routing protocol simplicity in exploitation interfaces, it's easy to integrate the routing protocol at intervals the prevailing operational systems, whereas not propelling the format of the header of the field messages.

4) OLSR protocol is compatible for the appliance that does not modify the long delays at intervals the transmission of the knowledge packets. the foremost effective in operation atmosphere for OLSR protocol could also be a dense network, where the foremost communication is concentrated between AN oversized form of nodes[15].

5)OLSR has collectively extensions to allow for hosts to possess multiple OLSR interface addresses and provide the external routing information giving the prospect for routing to the external addresses.

1.2.3 Dynamic provide Routing protocol (DSR)

The dynamic provide routing protocol (DSR) is associate on demand routing protocol. DSR is straightforward and economical routing protocol designed specifically to be utilized in multi-hop wireless unintentional networks of mobile nodes. The DSR protocol consists of two main mechanisms that job on to allow the invention and maintenance of route at intervals the unintentional network. Route discovery is that the mechanism by that a node S would like to send a packet to a destination node D obtains a route to D .Route discovery is utilized on condition that S tries to sent a packet to D and does not already grasp a route to D. Route maintenance is that the mechanism by that node S is in an exceedingly position to watch .while using a route to D if the constellation has changed such it'll not use it route to D as a results of a link on the route not works. once route maintenance indicates a route is broken. S can tries to use the opposite route it happens to know to D or it'll invoke route discovery all over again to hunt out a replacement route for resultant packets to D. route maintenance for this route is utilized on condition that S is de facto deed packets to D.

2. Two name and Trust theme in painter

In multihop networks like mobile impromptu networks stingy or misbehaving nodes will disrupt the full network and severely degrade network performance. Reputation, or trust primarily based models square measure one in every of the foremost promising approaches to enforce cooperation and discourage node actus reus. name is calculated through direct interactions with the nodes and/or indirect data collected from neighbours.

2.1 Shaping Trust

Trust (Reliability trust):- Trust is that the subjective likelihood by that a personal, A, expects that another individual, B, performs a given action on that its welfare depends.

2.2 Sort of Trust

There square measure 2 kinds of trust :-

Evaluation Trust:-Subjective likelihood by that a personal, A, expects that another individual, B, performs a given action on that its welfare depends

Decision Trust:-Willingness to rely on one thing or someone in an exceedingly given scenario with a sense of relative security, despite the fact that negative consequences square measure doable.

2.3 Side of Trust

This section describes totally different side associated with trust.

Trust Scope:-A perform that the relying party depends on and trusts

Functional Trust:-Trusted party performs the perform

Referral Trust:-Trusted party recommends a celebration which will perform the perform

Direct Trust:-Result of direct expertise

Indirect Trust:-Derived from recommendations

2.4 Shaping name

Reputation is formed and updated on time through direct observations and via information provided by totally different members of the community. name is formed and updated on time through direct observations and via information provided by totally different members of the community.

There square measure 3 styles of reputation:-

1) Subjective Reputation:-

The term subjective name to talk regarding the name calculated directly from a subject's observation. A subjective name at time t from subject si purpose of scan is calculated using a weighted mean of the observations' rating factors.

2) Indirect Reputation:-

The subjective name is evaluated exclusively considering the direct interaction between a topic matter and its neighbours. With the introduction of the indirect name live we've got a bent to feature the prospect to duplicate in our model a characteristic of advanced societies: the final word price given to the name of a topic matter is influenced to boot by information provided by totally different members of the community.

3) Purposeful Reputation:-

The term helpful name to talk regarding the subjective and indirect name calculated. the prospect to calculate a world price of a subject's name that takes into thought whole totally different observation/evaluation criteria.

Reputation could also be thought of as a collective live of trait supported the referrals or ratings from members terribly} very community. Associate in Nursing individual’s subjective trust could also be derived from a mixture of received referrals and personal experience. thus on avoid dependence and loops it's required that referrals be supported first hand experience exclusively, and not on totally different referrals.

3 Unsure Reasoning

Most tasks requiring intelligent behavior have some extent of uncertainty related to them. the sort of uncertainty which will occur in knowledge-based systems could also be caused by issues with the information. For example: knowledge can be missing or inaccessible,Data can be gift however unreliable or ambiguous because of measure errors.The illustration of the information could also be general or inconsistent.

Three ways of handling uncertainty:

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

3.1 Probabilistic reasoning

3.1.1 Classical Probability:

The oldest and best printed technique for managing uncertainty depends on classical math. enable USA to start to analysis it by introducing a few terms.

Sample space: take under consideration Associate in Nursing experiment whose outcome is not positive with certainty before. However, although the results of the experiment will not be noted before, all possible outcomes is believed. This set of all possible outcomes of Associate in Nursing experiment is believed as a result of the sample house of the experiment and denoted by S.

Event: any set E of the sample home is thought as an incident. That is, an incident may be a collection consisting of feasible outcomes of the experiment. If the results of the testing are contained in E, then we have a tendency to square measure spoken communication that E has occurred.

Mutually exclusive events: a gaggle of events E1, E2, ..., nut terribly} very sample house S, unit remarked as reciprocally selected events if $Ei \cap Ej = \emptyset$, $i \neq j, 1 \leq i, j \leq n$.

A formal theory of likelihood square measure usually created exploitation three axioms:

1) $0 \leq P(E) \leq$ one.

2) $\sum P(Ei) =$ one (or $P(S) =$ one

This axiom states that the whole of all events that do not have an impression on each other, remarked as reciprocally exclusive events, is 1.

3) P(E1U E2) = P(E1) + P(E2),

where E1 and E2 unit reciprocally exclusive events. In general, this may be collectively true.

3.1.2 Bayes' Theorem

Conditional probability is made public as

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

i.e., the prospect of H given E.

In real-life apply, the prospect P(H | E) cannot invariably be found at intervals the literature or obtained from maths analysis. The conditional prospects

$$P(E \mid H)$$

however usually unit easier to come back by;

Thus

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

Hypothetical reasoning as well as backward induction

1) Bayes' Theorem is sometimes applied for decision tree analysis of big business and conjointly the social sciences.

2) the strategy of theorem higher operation is to boot utilized in knowledgeable system labourer.

3.1.3 Theorem logical thinking

Is a technique of statistical inference in which Bayes' rules is wont to update the likelihood estimate for a hypothesis as additional evidence is non inheritable. theorem change is a crucial technique throughout statistics, and particularly in mathematical statistics. for a few cases, exhibiting a theorem derivation for a {statistical technique|statistical procedure|method} mechanically ensures that the strategy works still as any competitive method.[5]Bayesian change is particularly necessary within the dynamic analysis of a sequence of information. theorem logical thinking has found application in an exceedingly vary of fields as well as science, engineering, philosophy, medicine and law.

In the philosophy of decision theory, theorem logical thinking is closely associated with discussions of subjective likelihood, usually referred to as "Bayesian probability" theorem probability provides a rational method for change beliefs

Advantages and drawbacks of theorem ways

The theorem ways have variety of benefits that indicates their quality in uncertainty management. most vital is their sound theoretical foundation in applied math. Thus, they're presently the foremost mature of all of the uncertainty reasoning ways.

While theorem ways square measure additional developed than the opposite uncertainty ways, they're not while not faults.

3.1.4 Certainty issue

Certainty factor

Certainty issue is another methodology of handling uncertainty. This technique was firstly develop for the MYCIN system. One of the complexities with theorem methodology is that there unit too many possibilities required. Most of them could also be unknown. The problem gets really unhealthy once there unit many things of proof. Besides the matter of amassing all the conditional possibilities for the concept methodology, another major draw back that appeared with doctors was the association of belief and disbelief. ab initio sight, this might appear trivial since clearly disbelief is simply the choice of belief. In fact, the speculation of chance state

$$P(H) + P(H') = \text{one}$$

and so $$P(H) = \text{one} - P(H')$$

For the case of a posterior assumption that depends on proof,

$$P(H \mid E) = \text{one} - P(H' \mid E)$$

However, once the MYCIN knowledge engineers began interviewing doctors, they found that physicians were terribly reluctant to state their knowledge at intervals the sort.

The CF formalism has been quite trendy skilled system developers since its creation as a results of

1. it's a straightforward method model that permits specialists to estimate their confidence finally being drawn.

2. It permits the expression of belief and disbelief in each hypothesis, allowing the expression of the results of multiple sources of proof.

3. It permits knowledge to be captured terribly} very rule illustration whereas allowing the quantification of uncertainty.

4. The gathering of the CF values is significantly easier than the gathering of values for the other ways that. No math base is required - you just have to be compelled to raise the skilled for the values.

Other criticisms of this uncertainty reasoning methodology embody among others:

1. The CF lack theoretical foundation. Basically, the CF were part sudden. it's academic degree approximation of math.

2. Non-independent proof is expressed and combined exclusively by “chunking” it on among constant rule. once big quantities of non-independent proof ought to be expressed, this proves to be failing

3. The CF values could also be the choice of conditional possibilities.

3.1.5 Dempster-Shafer Theory

Here we've got a bent to debate another methodology for handling uncertainty. it's referred to as Dempster-Shafer theory. it's evolved throughout the Sixties and Nineteen Seventies through the efforts of Arthur Dempster and one in all his students, traveler Shafer.

1) This theory was designed as a mathematical theory of proof.

2) the event of the concept has been driven by the observation that math is not able to distinguish between uncertainty and knowledge as a results of incomplete information.

Frames of discernment: Given a set of potential parts, referred to as atmosphere,

$$\Theta = \{\Theta1, \Theta2, ..., \Theta n\}$$

that unit reciprocally exclusive and complete. The atmosphere is that the set of objects that unit of interest to U.S. The subsets of the atmosphere unit all potential valid answers throughout this universe of discourse. Associate in nursing atmosphere is to boot referred to as a frame of discernment. The term understands means that it's potential to differentiate the one correct answer from all the other potential answers to a problem. the flexibility set of the atmosphere (with 2N subsets for a set of size N) has as its parts all answers to the potential queries of the frame of 2 discernment.

Mass Functions and Ignorance: In theorem theory, the posterior chance changes as proof is acquired . Likewise in Dempster-Shafer theory, the idea conspicuous would possibly vary.It is customary in Dempster-Shafer theory to believe the degree of belief conspicuous as analogous to the mass of a object. That is, the mass of proof supports a belief. the principle for the Associate in Nursingalogy with AN object of mass is to place confidence in belief as a quantity which is able to move around, be go other ways, and combined. A basic distinction between Dempster-Shafer theory and math is that the treatment of knowledge. If you have no previous knowledge, then you wish to assume the chance P of each risk is

$$P=1/N$$

where N is that the variability of potentialities.The Dempster-Shafer theory does not force belief to be assigned to knowledge or refutation of a hypothesis. The mass is assigned exclusively to those subsets of the atmosphere thereto you'd wish to assign belief. Any belief that is not assigned to a specific set is taken under consideration no belief or nonbelief and easily associated with atmosphere □ . Belief that refutes a hypothesis is disbelief, that may not nonbelief.

Difficulty with the Dempster-Shafer theory

1) One downside with the Dempster-Shafer theory happens with standardisation and will cause results that unit contrary to our expectation.

2) the matter is that it ignores the idea that the factor being thought of does not exist.

4. Experimental Parameters

Throughput

It defines as a result of the whole vary of packets delivered over the whole simulation time.it is one in each of the dimensional parameters of the network that provides the fraction of the information rate used for useful transmission selects a destination at the beginning of the simulation i.e knowledge wheather or not data packet properly delivered to the destination[3].

Packet Delivery relation

Packet delivery relation is made public as a result of the relation of information packet received by the destination to those generation by the. Mathematically, it square measure usually printed as:

PDR=S1/S2

Where S1is the whole of information packet received by the each destination and S2 is that the whole of information packet generated by the each source[3].

End to complete delay

The average end to complete delay of information packet is that the interval between the knowledge packet generation time and thus the time once the last bit arrives at the destination.

The average time it takes a data packet to attain the destination[5].This includes all potential delays caused by buffering throughout route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at that initial packet was transmitted by provide from time at that initial data packet arrived to destination. Mathematically, it square measure usually printed as:

Avg EED=S/N

Where S is that the whole of the time spent to deliver packets for each destination , and N is that the vary of packet received by the all destination nodes.

Overhead

The amount of routing traffic increase as a result of the network grows. a vital of the quality of the protocol, and thus the network, is its routing overhead. it's printed as a result of the whole vary of routing packets transmitted over the network, expressed in bit per seconds or packets per second.

Some supplys of routing overhead throughout a network unit cited at intervals the vary of neighbors to the node and thus the vary of hops from the supply to the destination. various causes of overhead unit network congestion and route error packet.

5. CONCLUSION

MANETs include many little devices communication spontaneously over the air (wireless).The topology of the network is changing frequently as a result of the mobile nature of its nodes. specific finally induces that there don't seem to be any such things as mounted routers, thus every node should act as a router for its neighbors. Trust-based schemes area unit thought-about as effective mechanisms associated with cryptologic techniques for thwarting a spread of attacks. as a result of the properties of MANETs, trust establishment needs Associate in Nursing intelligent approach to identify attackers' misconduct.

A routing protocol for MANETs have to be compelled to offer incentives for acting properly and it have to be compelled to be able to realize misbehaving nodes and punish them. In MANETS no priori trust relationships and no central trustworthy authorities exist. The goal is to see trust relationships by using a reputation-based trust management theme. this could be done by getting name for a node and mixture this with personal observations regarding its behavior. theorem interface is utilized for direct observation and Dempster-shafer theory is utilized to calculate trust value supported indirect observation. to calculate trust price supported indirect observation.

6. 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] Velloso, Daniel de O. Pedro B. Cunha, Rafael P Laufer, Otto Carlos M.B. Duarte, 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.

[11] CHEN Aiguo, XU Guoai, Yang Yixian, “A Cluster Based Trust Model For Mobile Ad-hoc Networks”, 2008 IEEE.

[12] Y. Beghriche, V. Toubiana, and H. Labiod, “A bayesian filter to detect misbehaving nodes in manets,” in *Proc. NTMS’08*, (Tangier, Morocco), Nov. 2008.

[13] C. T. Nguyen, O. Camp, and S. Loiseau, “A Bayesian network based trust model for improving collaboration in mobile ad hoc networks,” in *Proc. IEEE Research, Innovation and Vision for the Future*, (Hanoi, Vietnam), Mar. 2007.

[14] Theodorakopoulos and J.S. Baras, “On Trust Models and Trust Evaluation Metrics for Ad-hoc Networks,” IEEE Journal on selected Areas in Communications, Vol24, No. 2, Feb 2006, pp. 318-328