Revisiting Trust Based Security Techniques in Wireless Network

Ritika Vishwakarma, Praful Pardhi

Abstract*: Trust establishment is a very critical issue in wireless networks. It demonstrates the use of various complex algorithms involved in creating a trust model, applying the model on each node of the network and verifying that the model is not attacked or compromised by trusted nodes. Various researchers have applied multiple algorithms to perform this task, each of the proposed algorithm has their own pros and cons when applied to a real time wireless network. This paper revisits some of the standard algorithms and tries to compare them in terms of efficiency and reliability, so that the readers of this text can get a sufficient level of understanding on which algorithms can be applied to which set of network parameters in order to improve the overall trust quality of the network. We also propose some interesting observations from our study to further enhance trust level of these systems.

Keywords: Trust level, attacks, model, verification, efficiency, reliability.

I. INTRODUCTION

Generally, independent PCs and little networks depend on client verification and access control to give security. These physical techniques use framework based controls to check the character of an individual or process, expressly empowering or confining the capacity to utilize, change, or view a PC asset. In any case, these techniques are deficient for the expanded adaptability that disseminated networks, for example, the Internet and unavoidable figuring conditions require in light of the fact that such frameworks need focal control and their clients are not all foreordained. Versatile clients hope to get to privately facilitated assets and administrations whenever and anyplace, prompting genuine security dangers and access control issues.

A wireless network is an unmistakable sort of network on account of its qualities, for example, no need of particular switches for sending the parcels and settled foundation. Itvery well may be sent and devastated in a fast time and nodes in this condition are moving uninhibitedly consequently making a dynamic topology. These qualities of A wireless network make it unique and offer a lot of uses very well may be sent and devastated in a fast time and nodes in this condition are moving uninhibitedly consequently making a dynamic topology. These qualities of A wireless network make it unique and offer a lot of uses.

Revised Manuscript Received on December 22, 2018.

Ritika Vishwakarma, Department of Computer Science, Ramdeobaba college of Engineering, India.
Prof. Praful Pardhi, Department of Computer Science, Ramdeobaba college of Engineering, India.

Anyway anchoring A wireless network is a paltry mission because of its own critical nature, for example, absence of concentrated control, open and shared wireless medium, unique topology, self-association and restricted asset obliges, for example, battery power, memory and absence of helpfulness. As of late, A wireless network has gotten huge consideration as a result of the self-design and self-support abilities. A major helplessness of A wireless network originates from open distributed engineering. Nodes in the network are completely needing different nodes to finish the information transmission effectively subsequently it doesn't depend on any devoted switches for sending the parcels, in its place every node goes about as a switch. Then again, wireless channel is available to both authentic network clients and noxious assailants. Therefore, there is no reasonable line of guard in MANETs from the security viewpoint. The nodes wandering in threatening condition with generally poor physical insurance have non immaterial likelihood of being endangered. Subsequently, we ought not limit ourselves to noxious assaults from outside the network, yet additionally consider the assaults propelled from inside the network by traded off nodes [1]. A wireless network is additionally powerful, due to visit changes in the two its topology and its enrollment. Trust relationship among nodes additionally changes; on the grounds that another node may join or leave and that node might be imperiled. The striking highlights of A wireless network present the two difficulties and openings in accomplishing security necessities [2], for example, Availability, Authentication, Non renouncement, Integrity, Authorization, Privacy and Confidentiality. Confirmation is a fundamental idea in the security point of view on the grounds that every node in the A wireless networkshould guarantee the character of the friend node with which it is imparting. When a confirmation is accomplished outstanding security objectives are not matter of concern. Along these lines to accomplish security, MANETs ought to have participation among the nodes and furthermore have a conveyed engineering with no focal elements. These qualities assist us with avoiding single purpose of disappointment.

Normally versatile specially appointed networks are famous for their abnormal attributes, for example, the absence of a changeless framework, the sporadic idea of availability, the progressively changing topology and the nonattendance of network wildernesses and focal substances [8]. Portable impromptu networks, because of their solitary qualities, request new

conventions and answers for their open issues, for example, reasonable steering conventions, advantageous QoS plans, pertinent network tending to plans and fitting security systems, for example. This work was bolstered to a limited extent by FDTE (Foundation for the Engineering Technological Development) - São Paulo - Brazil and Ericsson Research at Kista - Sweden. Leonardo A. Martucci was with Laboratory of Computer Architecture and Networks, Department of Computer and Digital Systems Engineering, Escola Politécnica, Universidade de Sao Paulo, São Paulo - SP, Brazil Security in versatile impromptu networks involves degree and condition as its prerequisites essentially rely upon the network reason and on the network objective. For example, the security prerequisites of a military specially appointed network vary as indicated by the confronted situation. Secrecy and accessibility are the most vital issues in a war zone, while in a helpful protect mission situation, accessibility is undeniably more important than privacy. Thusly, the application setting characterizes the security necessities for each situation.

As of late wireless networking has encountered exponential development. Utilization of wireless networking ranges the scope of human exercises from web keeping money to remote control of complex mechanical gear. There is little sign that this development will back off inside the following decade. The rising worldview of universal figuring has just powered the development. Universal processing alludes to a figuring model in which PC capacities are coordinated into individuals' every day life in an inconspicuous and straightforward way [1-4]. The pervasive model requires the connection of little cheap implanted PCs, wireless gadgets, and bigger PCs. Omnipresent processing encourages such things as home mechanization, for example programmed control of home apparatuses, remote programmed patient checking, and robotized sprinkler framework. An unmistakable however related networking model is the wireless sensor network. This is an "infrastructureless" or "impromptu" network of small scale, modest, low-control, multifunctional sensor nodes. These minor sensors nodes can perform detecting, information handling, and correspondence capacities [5]. A sensor node gadget for the most part comprises of five units: a power unit, a detecting unit, a handling unit, an information stockpiling unit, and a wireless handset unit [6]. Two imperative wireless sensor network upgrades over earlier sensors are: wireless sensor nodes can be situated in the genuine marvels (not at a separation), and sensor node organization and situating need not be pre-decided nor pre-designed [7]. The wireless sensor network is a one of a kind sort of specially appointed network, and can be connected in numerous fields [5]. In military applications, wireless sensor nodes can be quickly conveyed from flying machines or rockets behind adversary lines, and be utilized to lead combat zone reconnaissance. In flame ground applications, the wireless sensors might be utilized to measure the force of the fire (warm), track the course the fire is taking, or show how much the fire can develop by means of oxygen and additionally carbon readings. Wireless sensors can likewise be utilized to screen the dimensions of toxins in the climate and other ecological marvels. Utilizing wireless sensor networks to screen traveler developments at air terminals or to recognize atomic or natural assaults are manners by which these network can anticipate or 'early distinguish' demonstrations of fear mongering. In the medicinal field specialists can remotely screen patients' pulse and circulatory strain over a drawn out timeframe using wireless sensors. These wireless sensors could be inside or remotely connected to the human body. Brilliant sensor nodes can be implanted in home apparatuses to give property holders the ability of dealing with their machines locally or remotely through satellite or the web [5]. The conceivably immense uses of wireless sensor network clarify that it will be a noteworthy apparatus in the social event and dispersal of information. Because of the inalienable capability of wireless sensor networks to supply mission basic data continuously, there is an incredible need to make such networks secure. Notwithstanding, wireless sensor networks present one of a kind new difficulties which avoid coordinate use of conventional security systems [8]. For monetary practicality, wireless sensors nodes are restricted in power (typically can't be recharged), calculation abilities, transfer speed, and memory. The restriction of memory and preparing capacity make open key cryptography and advanced mark troublesome. What's more, the restricted intensity of these minor sensor nodes makes the correspondence overhead of customary security calculations unendurable. Sensor nodes are regularly sent in open zones, showing a danger of physical assaults since they connect intimately with the physical condition and individuals. This suggests wireless sensor nodes are presented to a more noteworthy risk than regular network nodes that are typically concealed in secure rooms [8].

II. NEED OF TRUST BASED SECURITY

Verification is a huge viewpoint in the security of A wireless network that empowers a node to guarantee the personality to the beneficiary [3]. As referenced before once confirmation is accomplished, rest of the security prerequisites could without much of a stretch be accomplished. To guarantee the confirmation every node must confide in different nodes. Thus a trust is a door and choice for versatile nodes to validate one another. Trust is a word which is initially gotten from the sociologies. Trust is characterized as "one element (trustor) is eager to rely upon another element (trustee) [4]" or "the trustor forsakes command over the activities performed by the trustee [5]". Basically, trust is dependence on an article or an element. As indicated by the network and correspondence field trust is characterized as "a lot of relations among

substances that partake in the convention which depends on the past association of elements inside the convention [6]". So as to finish the mission effectively every node ought to participate with one another. We can simply say every node has trust on different nodes. A wireless network is a decentralized circulated network. Consequently accomplishing helpfulness among the nodes is an entangled assignment. The reason is, every node in the network must confide in each other node any earlier proposals and collaborations. Be that as it may, this visual impairment in correspondence will make it progressively powerless against versatile nodes and influence the network execution extraordinarily. Consequently coordinating nodes must believe each other so as to accomplish the ideal security level. In addition contrasted and conventional wired network, gathering trust proof to assess a dependability of a specific node in A wireless network is critical issue because of its dynamic nature likewise another node may join or leave the network whenever [7]. Notwithstanding that, conventional cryptographic techniques are giving key based security where keys are pre-decided and furthermore rely upon any outsider consequently computational and network overhead drastically increment and it prompts execution corruption in by and large network's throughput, accessibility and power [8]. So as to defeat such issues trust appears. Trust is dynamic, the trust confirmations or data required for trust foundation may change because of its topology change consequently result might be off base or erroneous [9]. Trust is abstract that nodes in the A wireless network might not have same dimension of trust regarding different nodes in light of the fact that every node has diverse dimension of experience [10]. Trust is deficient and transitive that if A trusts B, B confides in C in the meantime A does not required to confide in C. For this situation transitivity among An and C depends on two things, for example, A trusts in C or A trusts in the C's suggestion of the outsiders [11]. Trust is unbalanced that every node has distinctive asset compel level so some higher limit node may not trust with lower limit node and the other way around [12] lastly trust is setting subordinate for example if a given errand requires high computational power, a node with high computational power is viewed as trusted in the meantime a node that has low computational power yet isn't vindictive is questioned [13].

With the exception of physical layer security, almost all security depends on cryptographic standards. Network security issues can be isolated into approximately four intently interlaced territories: mystery or classification, verification, non-revocation, and trustworthiness control [9]. Mystery has to do with making data unavailable to unapproved clients [9, 10]. Verification has to do with guaranteeing that the potential client is approved previously enabling that client to participate in the correspondence procedure [9, 10]. This is undifferentiated from an ATM PIN number that gifts one access to his/her cash subsequent to confirming learning of the PIN, which is thought to be known just by the approved client. Non-disavowal is comparable to signature. This is worried about guaranteeing that the data was sent from the source that it asserted sent it. How might you demonstrate that a letter really originated from your (CEO)? You could look at the organization seal alongside the mark of the supposed CEO to decide its realness. While you are certain that the organization seal and the CEO mark are legitimate, the substance of the letter may not be. It could have been effectively messed with by a middle of the road managerial staff. Honesty control tends to this worry with the goal that the substance of the data we get is the correct one sent by the source. Network security issues don't fit into one layer, however range nearly the whole Open System Interconnection (OSI) reference show convention stack [9]. Wireless correspondence is especially vulnerable to listening stealthily and recurrence sticking. Strategies to battle these include: encryption, spread range methods, and recurrence jumping. Notwithstanding, the greater part of the verified encryption calculations are improper because of the imperatives of wireless sensor nodes. The calculation necessity of these calculations is past the ability of the wireless sensor nodes. Likewise, at present, the memory of the wireless sensor nodes isn't sufficiently huge to store the cryptographic keys of numerous awry key calculations. At the information interface layer, parcels on a point-to-point line can be scrambled as they leave the source node and decoded at the goal node. Different blunder adjusting codes or plans can be utilized to successfully manage malignant impacts [9]. Research is continuous to create lightweight encryption methods for wireless sensor networks. In the network layer, firewalls can be introduced to channel through wanted parcels and square undesired bundles in conventional networks [10]. Be that as it may, the memory impediment of wireless sensor nodes makes the usage of bundle separating tables a test [11]. In the vehicle layer, whole associations can be encoded, start to finish (for example procedure to process). For greatest security this start to finish encryption is required. At last, issues, for example, verification and non-disavowal must be taken care of in the application layer. Nonetheless, in wireless sensor networks these objectives are trying to achieve, because of the absence of worldwide identifiers in many applications [5, 6].

III. TRUST BASED TECHNIQUES FOR WIRELESS NETWORKS

Analysts in [27] has a solid and organized various leveled trust demonstrate that uses the idea of computerized declarations for guards against pernicious nodes. This model pursues four stages, for example, issuing of endorsement, stockpiling authentication, declaration approval and repudiation of testaments. Here every one of the stages are executed locally by the nodes themselves aside from issuing of declarations. At the point when a node going into the network it communicates its testament to every one of the nodes in the network. Earlier, every one of the nodes ought to have a substantial computerized declaration issued by Certificate Authority (CA). Every node keeps up profile table which is utilized to decide if a given authentication is renounced or not. Each

profile table has a proprietor id, peer id, endorsement status and allegation data. On the off chance that any allegations found in the network, the data is about the allegations reliably kept up by each profile tables of the nodes. This procedure is enabling different nodes to discover the allegation node. To refresh data with respect to the denounced node, every node additionally keeps up a status table. At the point when an endorsement is renounced for a node, all recently settled trust connection for that node are being referred to, so node is promptly ignored by every one of the nodes and network get to is denied for that node.

While in [26] the analyst has proposed a NTM dynamic trust exchanges with a dynamic key assention plan to ensure the trust arrangement. It comprises of two segments. One is shared segment, it manages the safe correspondence with the neighboring nodes, for that every node has something like one network deliver declaration that will be utilized for validation which depends on the symmetric key. The second part named as remote segment which is in charge of trust arrangements and setting up secure start to finish correspondence. So as to achieve this every client has something like one personality authentication which is normally given by confided in outsider. The unlucky deficiencies of believed outsider amid exchanges are overwhelmed by three strategies, for example, testament renouncement list, probabilistic model and relegate load to the declarations. Remote segment is included with different sub parts, every one performing different exercises. Shared segment is utilized to secure the outer assailants and remote segment is utilized to ensure the inward aggressors.

Another fascinating work with regards to [28] has proposed a trust and notoriety based security engineering for DSR convention to distinguish the narrow minded nodes, to discover confided in courses and appropriation of trust. The trust display in this paper comprises of the accompanying three parts, trust operator, notoriety specialist and combiner. The obligation of trust operator is to determine coordinate trust estimations of its quick neighbors dependent on affirmation, bundle accuracy, unwarranted course answers, boycotts and rescuing. At that point the notoriety operators is utilized to share trust data about neighbors with different nodes by piggy sponsorship the immediate trust data of nodes onto the DSR control bundles while course ask for handling is completed. In course disclosure, the immediate trust data is shared either in the extra discretionary header of the control bundle or through adjustment of the current ROUTE REPLY control parcels. At long last the combiner operators process the last trust an incentive by blending the immediate trust esteem which is gotten from the immediate specialist and notoriety esteems by notoriety specialists. So as to register the dependable nodes, LINK CACHE component is utilized where trust esteem total and connection cost of every node is put away.

In [30] the scientists proposed a security trust observing layer to distinguish wormhole assault by analyzing proving ground on OLSR directing convention. The center idea of this model is Security Trust Monitoring (STM) where traffic analyzer, entomb correspondence of circulated STMs, trust race and approval, trust table and return confided in states modules are a piece of it. Each model plays out its one of a kind tasks. Traffic analyzer is utilized to ascertain nearby trust esteems by watching neighbors conduct. The determined nearby trusts are shared among the neighbors utilizing trust sharing system which is done in the between correspondence of conveyed STMs module and that sharing procedure is cultivated by intercommunication process. Trust race and approval module is utilized to approve the trust esteems and after the approval of trust those messages are called worldwide trust. Both the neighborhood and worldwide trust esteems are put away and dealt with by the trust table module. Last module is called trust to confided in express, this will happen when any node under examination that moves pernicious to suspicious or acting up to trusted.

A progressively advanced methodology was proposed in [29], where a half and half validation conspire which coordinates the dispersed confirmation with the affixed verification system. It has the accompanying stages, introduction of the networks, verification of new nodes and declaration reestablishment stages. In the principal stage expecting that every node in the network holds a couple of open and private keys additionally every node has an exceptional identifier IDi. Here RSA calculation assumes a critical job by giving System Public Key (SPK) and System Secret Key (SSK). The SSK is conveyed among N nodes by making utilization of Shamir Threshold Secret Sharing plan. These N nodes move toward becoming verification nodes. Every validation node holds a Secret Key (Ki) which is gotten by Galois field and Lagrange introduction equations. Also set of validation nodes can recoup the mystery by applying Lagrange insertion once more. In the second stage, another node discovers its one bounce neighbors for validation by asking for a question message. On the off chance that new node discovers enough confirmation nodes, it gets a System Certificate Key/SSK which is produced dependent on Lagrange insertion equation by verification nodes. On the off chance that it can't discover confirmation nodes from its one bounce neighborhood, it will approach some different nodes. Those nodes are past from its one jump neighborhood. Such nodes are called intermediary nodes. The intermediary nodes can discover enough validation nodes through trust exchange. Moreover another node confirms and can turn into an individual from the network. Testament recharging is utilized to safeguard against malignant nodes so every node reestablishes its authentications inside a particular timespan. It makes it difficult for noxious node to secure a mystery key. Declaration denial is required in two events first when the testament is released, Second authentication lapses for a specific node however the node does not issue another endorsement. It is reasonable for vast scale network in view of its versatility; the achievement proportion of verification is more.

An epic work portrayed in [33] proposes a security demonstrate that depends on trust and affiliation status of every neighboring node to keep the Gray Hole assault on unique source steering. Here the ideal is chosen dependent on the idea of relationship between the nodes not by the primary entry of course answer bundles. In this model, nodes are arranged into obscure, known and sidekick nodes and these are called affiliation esteems which depends on their trust and proper edge trust esteem. Obscure nodes are untrusted nodes with negligible trust esteems. Second buddy nodes are completely believed nodes with most extreme trust esteems. At long last, obscure nodes are middle of the road among known and buddy nodes. So as to store the affiliation esteems, affiliation table is utilized. By utilizing this table we can distinguish the vindictive nodes. Besides the estimations of affiliation tables may change because of node sending and getting exercises. Trust esteem is determined by including the apportion between the quantity of parcels really sent and number of bundles to be sent, proportion of number of parcels got from a node yet started from others to add up to number of parcels got from it and affirmation bit.

While in [32] the scientists proposed a security design for A wireless network through joint effort and trust instruments. In which the mischief nodes are distinguished by the Gossip based Outlier Detection calculation and dependable nodes are assessed by multi-dimensional trust the board. This anomaly calculation comprises of four stages, for example, nearby view arrangement, neighborhood see trade, neighborhood see refresh and worldwide view development. In addition neighborhood see refresh stage pursues two refresh strategies to be specific basic averaging strategy and trust based-weight technique. Every node produces its own nearby view by watching the neighbors conduct. Multi-dimensional trust foundation and the board are utilized to assess the node reliability from different viewpoints. These viewpoints in particular joint effort trust, social trust and reference trust. Community trust is utilized to pass judgment on how the node is taking an interest in the network exercises. Social trust is gotten from the nodes unusual practices lastly reference trust is gotten from different nodes feeling about the objective node.

A quite certain trust show was proposed in [35] which have a trust based security for OLSR steering convention developed on trust determination dialect. Likewise offered trust based thinking to enable every node to assess the conduct of different nodes. Ordinarily, this model comprises of three stages, neighborhood choice, Multi-Point Relays (MPR) choice and steering table figuring. MPR are chosen nodes that forward communicate messages in the network. Trust foundation is completed in the area revelation stage itself utilizing the trust particular dialect alongside the HELLO message. The second stage is MPR choice that nodes with least number of neighbors empowering it to achieve all the two jump neighbors those nodes are called MPR nodes. This stage likewise pursues the trust determination dialect to build up trust with the assistance of TC message. In the directing table count, a node figures the most limited way utilizing Dijkstra briefest way calculation likewise with the assistance of trust detail dialect. Trust based thinking is utilized to approve the area revelation by whether the area nodes experienced the trust particular dialect and furthermore is utilized to approve the MRP choice by checking the TC message and information parcels age.

Scientists in [34] proposed a dynamic trust forecast model to assess the dependability by nodes chronicled conduct just as nodes future conduct through expanded fluffy rationale rules expectation. This model incorporated into the source steering component and frame Trust based Source Routing convention (TSR) to pick a most limited course with security. The trust forecast model takes nodes recorded trust, nodes current trust and course trust into record for assessing the last trust. In TSR, course disclosure is cultivated with the assistance of FLOW-REQ message and course support is completed when course refresh, course handoff, node versatility and course mistake happens. Every one of these exercises depend on the trust forecast instrument.

IV. ANALYSIS AND CONCLUSION

Security is an imperative research region in the field of wireless network due to its extraordinary qualities. Accomplishing security prerequisites in a wireless network in a dynamic just as open framework is excessively troublesome. So as to accomplish the security level, every node must guarantee the personality of the companion node. Trust is a key to give a choice in the dynamic condition to every node to confide in different nodes. From this audit we presume that the greater part of the trust put together securities are based with respect to immediate and aberrant or proposal esteems from nodes of the networks and this trust data is joined with customary security techniques, for example, testament and key administration. As saw from the going with table, CONFIDANT tradition the attacker can send false aware messages of isolate a fair hub by affirming it as an awful hub. The ambushes like wormhole, emulate, Sybil strike, etc still exists in a part of the tradition, for instance, trusted AODV, CONFIDANT. As in CONFIDANT tradition the reputation of a hub is extended when it progresses he group so the poisonous hub that influence wormhole to get high reputation regard. Most of the traditions like TDSR, SRT, etc think about some as execution structures like pack pass on ratio(no of compelling packages/no of groups sent), ordinary from beginning to end delay to advance bundles to the objective and find back solution, correspondence overhead, course decision time, throughput, etc. to check the execution. These traditions simply focus on the improvement of the execution through trust frameworks anyway don't focus on the security flaws pushed by toxic hubs on the system. A couple of traditions, for instance, FrAODV, FACES constructs correspondence overhead in view of inordinate calculation for course finding and periodic flooding of control bundles.

The following table summarizes the protocols and their properties,

Protocol name	Pros	Cons
Trusted Ad Hoc on Demand Distance Vector (TAODV)	1) It can recognize noxious hub and narrow minded hub in system 2) It is more secure and having preferable execution over AODV 3) It can avoid change, creation assaults	1) It has no confirmation component of hubs and messages 2)It can't counteract worm-gap and pantomime assault
Cooperation Of Nodes: Fairness In Dynamic Ad-Hoc Networks (CONFIDANT)	Thisprotocol successfully distinguish childish hubs and PM wormhole hubs that drop bundles	1) It can't counteract different assaults, for example, alteration pantomime creation Sybil assault by noxious hubs 2) An assailant can send false caution messages and can do false guarantee that a hub is getting out of hand.
Friendship Based Ad Hoc On Demand Distance Vector (FrAODV)	Better QoS administrations like bundle conveyance part, standardized directing burden	The communication delay is higher
Trusted AOMDV	Execution is estimated as far as course choice time, trust bargain with TDSR,AOMDV and so forth	This convention estimates the execution in fixed portability condition that really not relevant in MANET
Friend Based Ad Hoc Routing Using Challenges To Establish Security (FACES)	Test parcel recognizes flooding, dark gap, parodying, alteration, dropping of control bundles. Just as it gives better execution within the sight of malevolent hubs.	In this convention control overhead is expanded because of intermittent flooding of test parcel and occasional sharing of companion list
Trust Based Security Protocol(TMSP)	This convention keeps up privacy and confirms the hubs dependent on computerized mark. It recognizes the hubs which are getting rowdy.	Can't identify validated pernicious hub. Expands control overhead
Trust Based DSR	Better throughput	High Delay, Low PDR

V. FUTURE WORK

As machine learning and AI are gathering a lot of momentum, and blockchain technologies are coming up very rapidly, researchers can combine machine learning and AI with blockchain in order to improve the overall trust level of the system with the help of a fully P2P protocol which reduces dependency on a central node, and improves the quality of the network via a better trust system.

REFERENCES

1. Huang, J., Woungang, I., Chao, H., Obidant, M., Chi, T., Dhurandher, S.K.: Multi-Path Trust –Based Secure Aomdv Routing In Ad Hoc Networks. Ieee 2011
2. S Sivagurunathan, V Mohan and P Subathra, "Distributed Trust Based Authentication Scheme in A Clustered Environment Using Threshold Cryptography for Vehicular Ad Hoc Networks," International Journal of Business Data and Communication and Networking (IJBDCN), vol. 6 (2), 2010.
3. S. Buchegger, J. L. Boudec, (2002) "Performance Analysis Of Confidant Protocol", Mobihoc'02, Epfl Lausanne, Switzerland, Pp226-236.
4. Yannick Lacharite, Dang Quan Nguyen,Maoyu Wang and Louise Lamont, " A Trust-based Security Architecture for Tactical MANET," Crown,2008.
5. Asad Amir Pirzada, Amitava Datta and Chris Mcdonald, "Incorporating Trust and Reputation in the DSR protocol for Dependable Routing," pp.2806-2821, Elsevier, 2006.
6. H. Rutvij, Jhaveri, D. Ashish, Patel, D. Jatin, Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV," International Journal of Computer Science and Network Security, vol.10 (4), 2010.
7. Bamberger and Walter, "Interpersonal Trust – Attempt of a Definition," Scientific Report, 2010.
8. W J Adams, G C Hadjichristofi and N J Davis, "Calculating a Node's Reputation in a Mobile Ad Hoc Network," Proc. 24th IEEE Int'l Performance Computing and Communications Conference, pp. 303-307, 2005.
9. William Stallings, Cryptography and Network Security., Pearson Education, 2003.
10. Neetu Singh Chouhan and Shweta Yadav, "Flooding Attacks Prevention in MANET," International Journal of Computer Technology and Electronics Engineering, vol. 1(3), 2011.
11. K Sivakumar and G Selvaraj, "Overview of Various Attacks in ANET and Countermeasures for Attacks," International Journal of Computer Science and Management Research, vol. 2(1), 2013.
12. Dhurandher, S.K., Obidant, M.S., Verma, K., Gupta, P., Dhuradar, P.:Faces: Friendhip-Based Ad Hoc Routing Using Challenges To Establish Security In Manets Systems. Ieee System Journal, Vol.5, No. 2, June 2011
13. Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANETInternet Communication," International Journal of Computer Science and Security, vol. 4(3), 2010.
14. A. M. Pushpa, (2009) "Trust Based Secure Routing In Aodv Routing Protocol", International Conference On Internet Multimedia Services Architecture And Applications (Imsaa), Usa: Ieee Press, 1-6.
15. P T Tharani, K Muthupriya and C Timotta, "Secured Consistent Network For Coping Up With Fabrication Attack in MANET," International Journal of Emerging Technology and Advanced Engineering, vol. 3(1), 2013.
16. Asma Adnane, Christophe Bidan, Rafael and Timoteo de Sousa Junior, "Trust based security for the OLSR Routing Protocol," Elsevier, 2013.
17. Y L Sun, W Yu, Z Han, and K J R

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Sel. Areas Communication, vol.24(2), pp. 305-317, 2006.
18. Wei Gong, Zhiyang You, Danning Chen, Xibin Zhao, Ming Gu and Kwok-Yan Lam, "Trust based Malicious Nodes Detection in MANET," IEEE,2009.
19. Bhalaji N and Shanmugam A, "Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Ad Hoc Networks," Elsevier, 2012.
20. Raja Rai Sign Verma, Donal O' Mahony and Hitesh Tewari, "NTM-Progressive Trust Negotiation in Ad Hoc Networks," Proceedings of the 1st Joint IEI/IEE Symposium on Telecommunications Systems Research, 2001.
21. A Abdul-Rahman and S Hailes, "Using Recommendations for Managing Trust in Distributed Systems," Proc. IEEE Malaysia Int'l Conf.on Communication, 1997.
22. Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," IEEE Communications Surveys & Tutorials, vol. 13(4), 2011.
23. Wei Gong, Zhiyang You,Danning Chen, Xibin Zhao,Ming Gu and Kwok-Yan Lam, "Trust based Malicious nodes Detection in MANET," IEEE, 2009.
24. Akanksha Saini, and Harish Kumar, "Comparison between Various Black Hole Detection Techniques in MANET," National Conference on Computational Instrumentation, 2010.
25. Edua Elizabeth, N., Radha, S., Priyadarshini, S., Jayasree, S., Naga Swathi, K.:Srt- Secure Routing Using Trust Levels In Manets. European Journal Of Scientific Research, Issn 1450-216x Vol. 75, No. 3 (2012), Pp. 409-422
26. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, "SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks," IEEE, 2008.
27. Essia, T., Razak, A., Khokhar, R.S., Samian, N.: Trust-Based Routing Mechanism In Manet: Design And Implementation. Springer, 18 June 2011.
28. M B Mukesh Krishnan, P Sheik Abdul Khader, "Fuzzy Based Security Model to Detect Compromised and Selfish Nodes to Mobile AD HOC Network," European Journal of Scientific Research, vol. 86(4), pp. 520-524, 2012.
29. L Eschenauer, V D Gligor and J Baras, "On Trust Establishment in Mobile Ad Hoc Networks," 10th Int'l Security Protocols Workshop, vol. 2845, pp. 47-66, 2002.
30. Ngai, Edith Ch and Michael R. Lyu, "An Authentication Service based on Trust and Clustering in Wireless ad hoc Networks: Description and Security Evaluation," IEEE, 2006.
31. Carlton R Davis, "A Localized Trust Management Scheme for Ad Hoc Networks," Proceedings of the 3rd International Conference on Networking, 2004.
32. R C Mayer, J H Davis and F D Schoorman, "An Integrative Model of Organizational Trust-Academy of Management Review," vol. 20 (3), pp. 709-734, 1995.
33. Guojun Wang, Qiong Wang, Jiannong Cao and Minyi Guo, "An Effective Trust Establishment Scheme for Authentication in Mobile Ad Hoc Networks," IEEE, 2007.
34. Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks," Proceedings of the World Congress on Engineering and Computer Science, 2008.
35. Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, "A Survey on Attacks and Counter measures in Mobile Ad Hoc Networks," Springer, 2006.
36. J S Baras and T Jiang, "Managing Trust in Self-Organized Mobile Ad Hoc Networks," Proc. 12th Annual Network and Distributed ystem Security Symposium Workshop, 2005.
37. Wenjia Li,James Parker and Anupam Joshi, " Security through Collaboration and Trust in MANETs," Springer, 2010.
38. S Staab (Editor), "The Pudding of Trust," IEEE Intelligent Systems, vol. 19(5), pp. 74-88, 2004.
39. Sharma, S., Mishra, R., Kaur, I.: New Trust Based Security Approach For Ad-Hoc Networks .Ieee(2010)
40. Arif Sari1 and Beran Necat, "Securing Mobile Ad-Hoc Networks Against Jamming Attacks through Unified Security Mechanism," International Journal of Ad Hoc, Sensor & Ubiquitous Computing, vol. 3(3), 2012.
41. Hui Xia, Zhiping Jia, Xin Li,Lei Ju and Edwin H.M.Sha, " Trust Prediction and Trust based Source Routing in Mobile Ad Hoc Networks," Elsevier,2012.
42. Bhalaji, N., Mukherjee, D., Banerjee, N., Shanmugam, A.:Direct Trust Estimated On Demand Protocol For Secured Routing In Mobile Ad-Hoc Networks. International Journal Of Computer Science & Security, Vol. 1, Issue (5)
43. Vinay P.Virada, "Intrusion Detection System (IDS) for Secure MANETs- A Study," International Journal of Computational Engineering Research, vol. 2(6), pp. 75-79, 2012.
44. G. Aggelou (2004) Mobile Ad Hoc Networks, Mcgraw-Hill.