A Self-Assurance Method Based on Trust Estimation for Secure Routing in MANET

T.Shekar Reddy, Y.RamaDevi

Abstract: ***The improved edition of conventional wireless networks provides a mobile temporary network (MANET), which is extremely appropriate for urgent situations. However, in a similar instance, its infra-low and resource limit creates many challenges in its performance. The growing security risks are probable to take place due to dynamic behavior and the absolute communication cycle which are based on unnoticed nodes, which dropped packets as they desire. Reliable and trusted nodes can reduce communications overhead and many past security schemes have suggested that high turnover can be achieved. Several security studies are expected to be trustworthy and less expensive. This paper aims to propose a self-assured approach (SAA) based on trust assessment for secure routing to secure high-security constancy and security for reliable database delivery based probability assessment. The assessment will be evaluated and the node maintains and identifies among random momentary errors and deliberate malicious actions and asses a node total trustworthiness to have secure and safe communication.***

Keywords: Secure routing, Trust estimation, Self-Assurance, MANET.

I. INTRODUCTION

Wireless communication equipment and network advancement offer the ability to connect dynamically to construct a short-term network known as MANET. Each node acting on a network such as an intermediate router and full dialogue depends on randomly changing topology, which mostly not able to provide confirm the guarantee of the delivery certainty. The randomness of route discovery in routing not guarantee harmful nodes. Information protocols used in the sense that all participants are loyal to the meetings. However, users who misbehave in a trusted communication environment can cause harm or other honest methods to opt-out of network performance. Thus, the nodes are entirely dependent on the safe route for successful packet transportation, to ensure effective utilization in a wireless temporary network, especially the crucial question. A non-assurance node such as Malicious or selfish nodes [5], [20] is always aimed at utilizing an additional network and its sources or deliberately producing fake-node details related to general nodes. The majority characteristic nodes are trying to obstruct most of the data routing channel that needs less bandwidth, which can reduce the device's resource source to reject the routing packet.

Various types of attacks include traffic, denial of service, a way of imagination, [2], [18] making malicious nodes (MAL-Node) targets that affect all communication operations. This type of selfish and malicious broadcasting creates a serious problem in the conversation.The most traditional methods able to make out the self-seeking and harmful node in respect of the understanding of the packet drop, however, a node may have the different conditions for packet losses, based on this assumption that this technology is punitive or away from the network. This makes the depreciation of the trustiness and reduces the belief of a node and, later eliminated from the network, a major defect of traditional technology [7]. The effect of changing the Node Behavior (N-Behavior) in experimental data routing affects the dilemma of a risk-free node for solving the problem. Utilizing a two-factor estimation relies on responses of the transmitting and receiving of the packets in the previous system approaches [4], [10]. This can increases network supervision overhead and resulting in a higher instability and low performance [9], [29].

However, to our understanding, there is a few efforts to evaluate the character of the node. The paths of MAL-Nodes relies on node connection and packet forwarding to eliminate MAL-Nodes [4], [11].

But these functions unable to analyze the impact of the node based on definite events on network constancy. The objective of this proposal is to resolve this issue through the "Node Trust Recovery Mechanism" to secure long-term network stability for

reliable and high packet delivery. This paper proposed a "Self-Assurance Approach (SAA)" to overcome the trust assessment limitation of nodes. Evaluating node performance is a key factor in determining the reliability and future forecasts of a node. It provides a node guarantee and declares that it is as harmful as falling security packets. The strength of the proposal is that it provides a clear distinction between selfish, vulnerable, and public nodes to provide a reliable and trustworthy node that builds a stable and secure network.

The structure of this article is structure as given below. In Section 2, it explains the work associated with the importance of node activities and secure routing based on trust characteristics. In Section 3, we explain the proposed Self-Assurance estimation method and Section 4 illustrates the experiment and result evaluation. In the last section, we provide a conclusion of the paper.

II. RELATED WORKS

The past studies by the various researchers have discussed the network firmness in the form of diverse perspectives [1], [2], [10], [12], [13], [14].

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author

T.Shekar Reddy*, Assistant Professor in Department Computer Science at University College for women(A), Osmania University.

Y.RamaDevi, Ph.D in Computer Science and Engineering from Central University of Hyderabad, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

It defines the concept of network existence based on the network traffic related with conventional communication networks and services, all of which focus on network authentication and node silence [15], [30]. It explores two key areas of a promising network, such as trusted communications and trusted operating systems for network stability [22].

In the past, many proposals are presented related to wireless security based on trust to improvise the security gaps [2], [6], [10], [12].

Here, most proposals monitoring their neighboring node activity for assessment of trust through direct observation [23], [24]. [25], [33]. It will define the malicious behavior of a node relies on the a range of forwarding packets received by its neighbors. The source node calculates the credible value by directly identifying any packet modification made by the intermediate node in the path [18]. An indirect approach given trustworthy consideration is to update the positive or negative actions of a node relies on messages received by neighboring nodes or range nodes. This assessment will be considered to redefine trust and remove MAL-Nodes [13], [17], [26], [27], [31]. Typically, wireless node monitors neighboring node operations such as "Packet Transmission", "Loss of Packet" and "Network Link" for guaranteed packet delivery, but all these actions unable to describe N-Behavior. The authors of [16] discussed the impact of indirect inspections on node dissemination. A MAL-Node can reduce the trustworthiness of a standard node by promoting a negative information and restore node trust by promoting a positive information. Analyzing the trust method directly or indirectly will help reduce the number of messages that affect the recovery plan to prevent the limitation of the computation in the trust.

Due to "low trust", active nodes cannot access, new unstable nodes which cannot connect to the network, so recent operations are not monitored and node recovery is inadequate [16], [21]. Marchang et al, [3] recommend IDS which is an effective plan to analyze and optimize the period of active activity in MANET. An experimental model has been proposed to reduce each operating time by using the collaboration between IDs between the nodes. Z. Movahedi et al. [1] offer a complete perspective of different trust supervision frameworks that fit into MANET and is able to hold misguided and critical current attacks to count on confidence to misinform trust-based network process identified as trust alteration attacks. It proposes to categorize key-tracked trusted traffic attacks based on how nodes can predict the guarantee of other nodes.

K. Ullah et al. [2] focused on research trusts and security concerns to develop security guarantees in MANET. In summary, it suggests a secure trust model that influences the key adherence to security guarantee and trusted communications and proposes a trust metric based on the dynamic action of dynamic scenario nodes. S.A. Thorat et al. [4] match up to the trust with utilizing cryptosystems for MANET routing safety. It cites a "trust-based routing protocol" in MANET design details. Jenitha T. et al. [24] has recommended an enhanced method to select a trusted node for participating in the main production processes of communication groups in the MANET environment to be delivered. P.Narula et al. [8] demonstrate a "Trust-based Multipath Routing (TMR)" uses the message security method to deliver trust-based routing. This method reduces the number of packets in cryptographic mode during less trust assured nodes", so a MAL-Node is corrupted and more routing strategies using trusted levels are the most "scalable routing" offers and these are on the path away from the trusted nodes.

Dhurandher et al. [28] demonstrate a Friend Based Ad-hoc Routing knows as "FACES" employing confronts to set up a security and loyalty routing in MANET. It defines a mechanism to build a protected network employing a set of Friends Lists (FL), that distributes this FL in the network of companions. Friends are analyzed and founded on the data transfers accomplishment among other friends' nodes in the network. Every one node has time to implement a method to obtain an FL of distribution partners and construct node responsibilities of partners. Depending on this intervallic update, MAL-Nodes able to with no trouble eliminated from the network. This procedure did not require neighboring broadcasts to evaluate node assurance. The disadvantage of this proposal is delayed due to the malicious behavior of computational overload and FL nodes, which affects the complete FL of friends, and communication and network constancy.

Even though the negative action of the node in the present circumstances has a direct impact on the node's trust, it is good to provide a recovery option, although it has a negative history and is expected to account for current needs. It is possible for bad or harmful nodes when affecting trusted nodes. Based on the importance of the observation and guarantee system's node and the importance of trust properties we proposed a Self-Assurance Approach as discussed in the following section.

III. PROPOSES SELF-ASSURANCE APPROACH

A Self-Assurance Approach (SAA) deals with an assessment of the node attribute and identity to participate in the network [32]. As mentioned on top of, N-Behavior is a significant feature in assessing the node trust. Nodes were able to handle both approaches: "*assured*" or "*non-assured*". However, the reason for this behavior is created to obstruct the network guarantee. This suggestion deals with a novel N-Behavior assessment algorithm that assesses and estimates a behavioral grouping that uses an efficient "Decision-Making" scheme for node trust managing and constant data transmission in MANET.

A. Categorization of Node Conducts

In MANET routing are relies on the intermediate nodes collaboration and their trust. This is an essential procedure in MANET, which must be managed to complete data transmission [12]. Every node on the network works on a personal mechanism and individual system. They have full freedom to determine their actions and reactions based on two classification factors as,

- **Assured Category (AC):** This category of node action supports all routing rules as a best effort to provide control and data packets and discovers the accurate path for proficient routing.

In general operations, the behavioral assessment algorithm is used to classify the exact N-Behavior category estimates based on the action classification on which the probability assessment is used.

B. Self-Assurance Based on the Trust Computation

The MANET feature in the actual instance is accidentally changed at several instances for various causes. This makes the N-Behavior random at every occasion in the actual-instant network. This may as well cause some attacks or resources required to sustain network strikes and packet forwarding. It evaluates the behavior of dissimilar groups regarding changes made to the following observations.

- Due to energy loss and misinformation, they may affect the node affecting the promise of failure and other malicious attacks or self-esteem that protect its sources.
- Appropriate reconstruction able to as well re-establish the trustworthiness of "selfish" or "harmful nodes". This reconstruction may be negative or failing to reduce energy sources.
- A MAL-Node may be an unsuccessful node, however, if the malicious behavior does not go wrong, it is no extensive believed reliable or self-reliant.
- If the unsuccessful node routing operations are at regular intervals constant, the node is once more believed.

Even though there is no special cause to perform transforms in the top of estimates, this makes the observed modify of the most widespread network scenes more common. To simplify this hypothesis to measure accurate expectations, we use the probability assessment [11] to get a mathematical model. Let the concept of the network area containing the N nodes containing the different categories as, S of nodes mentioned above. It represents S = *{"AC", "NA"}*. Especially in a time interval, T these nodes can simultaneously change behavior in S, which is represented as,

$$S = \int_{n=0}^{N} T(Prob\ ['AC', 'NA']) \tag{1}$$

The possibility of these behavioral modifies able to be assessed as, E_n , at a course of the instance as, C_n and where, C_n S, can be given as,

$$E_n = prob\ ((E_{n+1} \rightarrow C_{n+1}) \mid (E_n \rightarrow C_n)) \tag{2}$$

The Estimation based on the Equation (2) for a Probability Estimation [11] in the area S for all nodes N as E_n, and where "$n = (0,1,2, \ldots ,n)$". On the other hand, the dynamic behavior of the node transforms entirely into the inspection series. In the end, the node's behavior node of the present node, *t(n)*, classifies the future of the categories. For example, "C_n is a present state of a node" and after a time, t the behavioral conduct alter from "$C_n = C_n +1$", and it determinate to be correlated through a Probability estimation value as,

- **Non-Assured Category (NA):** This kind of node activity is unstable as a result of the network being "inconsistent", "high traffic", and "frequent link failures".

$$M_{a,b}\ (C) = Prob\ (\ P_{n+1} = b,\ C_n \leq c \mid P_n = a) = p_{ab}\ T_{ab}(c) \tag{3}$$

where, "$p_{ab} = lim_{s \rightarrow \infty}$" and "$M_{a,b}\ (C) = Prob\ (\ P_{n+1} = b \mid P_n = a)$", symbolizes the alteration of conducts probability between the node "*a*" and "*b*", and "$T_{jkab}(c) = Prob\ (P_n \leq c \mid P_{n+1} = b,\ P_n = a)$", correspond to time period among two type alter between the node *"a"* and *"b"*. On the source of dissimilar classification conduct alterations of a node, a probability matrix is offered in Table 1.

TABLE I. The Prospect Of Node Conducts

	AC	*NA*
Non-Malicious	1	0
Malicious	0	1

The probability of Behavior transforms using this matrix Table-1, it was able to approximate the behavior of the node relative to the current time of the distribution, "$T_{ab}\ (t) = 1 \mid 0$". A node does not modify when delivering behavior and latest behavior, and if the alter at one moment is measured, the prospect of the modify is measured zero. Futuristic definition models for nodes are self-efficacy based on these estimates. This assessment model has been used to assess the evaluation and sets up safe and trusted communication.

Individual node trust calculations usually maintain individual operations, for example, data transmission and request processing [24]. Reliability or collective assurance trusts *(CAT)* can be trusted of A_{Trust} in beside the person conducting it. In relates entity behavior trusts, it describes compilation trusts to review whether or not neighboring nodes are harmful. Accumulatively trusts are determined from personal conduct trusts. There are a lot of traditions to calculate the Accumulatively Assurance Trust [12], [17], [18], [19], it suggests the node *i* as "CAT_i". Node trusts are calculated based on individual amount guarantee trust (*TATs*) through the nodes over time. Each node has 1 maximum mass reliability value. [1] Between "0" and "1", trusted series for together A_{Trust} and *CAT* are among "0" and "1", the best *CAT* for a node able to estimate utilizing Equation (4) below.

$$CAT_i = TAT_i \times A_{Trust}\ (i) \tag{4}$$

In case of a node's t_{rust} is small, then the scheme will reduce the collective properties and the threshold drops to the bottom. Hence, A_{Trust} effects affect the cumulative trusts that hold certain credentials. Every action used by the node is calculated after the conversion Eq. (4), you can turn out job-depended on the action-based improvement for the N-Behavior investigation and trust re-establishment opportunity.

Retrieval Number: F4380049620/2020©BEIESP
DOI: 10.35940/ijitee.F4380.049620

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. EXPERIMENT EVALUATION

The proposed Self-Assurance Approach (SAA) it relies on the Trust to meet the circumstances discussed in division-3 and implemented through a MANET routing setting. This testing seeks to assess the probable events and behavior of the basic and intermediate nodes in opposition to the various packets transmitted to the receiver node for the counts of packets transmit from the source node. It demonstrated efficient use of A_{Trust} by modifying an AODV routing protocol.

A.Experiment Setup

A simulation analysis was done using the "GlomoSim" network simulator. It presents a standardized allotment of nodes and additional realistic progress patterns. However, as prescribed, the speed is distributed in a single-way model with the same mode of motion. Also, modification of their behavior as per the simulation, instruction node. AODV is being utilized as a routing protocol for trusted nodes, but revised versions from AODV's fraudulent nodes develop and are not following routing and forwarding rules found in their behavior.

TABLE II. SIMULATION FACTORS

Configuration	Parameter Values
Simulation Time	1000s
Simulation Area	1500m X 1500m
No. of Nodes	100
Mobility	RWP
Mobility Speed	0 to 20 m/s
Pause Time	30s
Packet Size	512 bytes
CBR Rate	4pkts/s
Minimum A_{Trust}	0.6
Malicious Nodes	10, 20, 30, 40, 50

In particular, the "non-existent nodes" future "RREQ" and "RREP" messages will not come forward to others. The MAL-Nodes transmitting "RREQ" and "RREP" information's, however, it drops the transmitted data packet. Resulting in the standard importance of many additional harmful nodes in the simulation iterations. The simulation runs for 600 sec, utilizing the configuration factors for network settings as presented in Table 2.

A. Result Analysis

In this section, the proposed SAA's AODV [14], TMR [8] and FACE [28] and trust-based routing mechanism are based. We estimate a MAL-Node differently and then evaluate the Trusted assurance Limit (ATRust) to measure the result of the simulated parameter configuration given in Table 2. In this section, it measures up the achievement of proposed "SAA with AODV" [14], "TMR" [8] and "FACE" [28], which routing mechanism rely on the trust evaluation.

First and foremost, it estimates the achievement by altering MAL-Node and afterward altering the threshold for the trust assurance (A_{Trust}) to compute the outcome of the simulation parameter configuration given in Table 2. The outcome of the MAL-Node is monitored by a trusted node and the diverse parameters are measured and the outcome values are as follows.

- **Throughput:** It is computed relies on the "*number of a packet transmitted*" upon the "*number of packets delivered*". In Fig.1, executable performance is measured. Comparison results can be improved on AODV, FACE, and TMR, which are the number of variants of MAL-Nodes. Increasingly, harmful nodes influence the network outflow by reducing the packets. Today's technology usually penalizes the whole node in case of loss of case packets, even if they are guiltless. Each decision-making approach and its past collective trust assesses the SAA's exemption for each sentence, which helps in retaining and improving pathways. Accurate estimates permit nodes to return to the network to balanced and provide good backup.

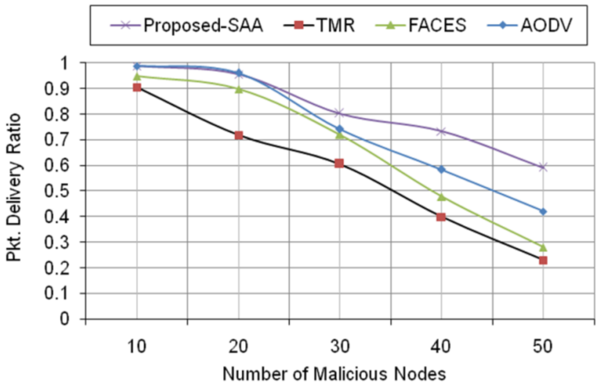

Fig.1. Throughput Performance Comparison

- **Packet Dropped:** It is computed based on the summation of packets drops during a particular simulation. Fig.2 shows the various packets that have been ignored for the number of MAL-Nodes. In case of an increase in harmful nodes, "AODV" and "FACES" illustrate excessive packet failure due to high DoS by the MAL-Nodes and routing route. The proposed SAA method agrees to the node to re-establish its trust and maintain extreme packet transmission and low packet drops.

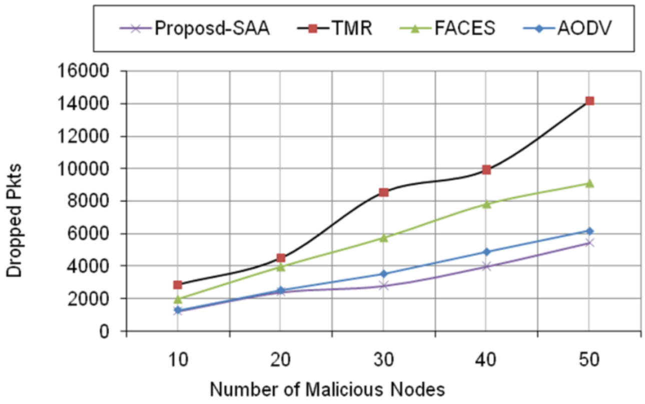

Fig.2. Packet drop Comparison

- **Control Overhead:** It is computed utilizing the entire number of control packets transmitted for each iteration of the simulation. In Fig.3, demonstrates the assessment of the protocol control overhead. All protocols have achieved an important order of increase in the various MAL-Nodes.

The presence of a high MAL-Nodes increases the loss of data packets, which causes a high overhead and low throughput, where the "FACES", "TMR", and SAA contrasts the contrast to maintain a trustworthy node through the behavior prediction. In both protocols, estimating intermittent node assurance ensures that they are safe and support packet loss and reduce control overhead.

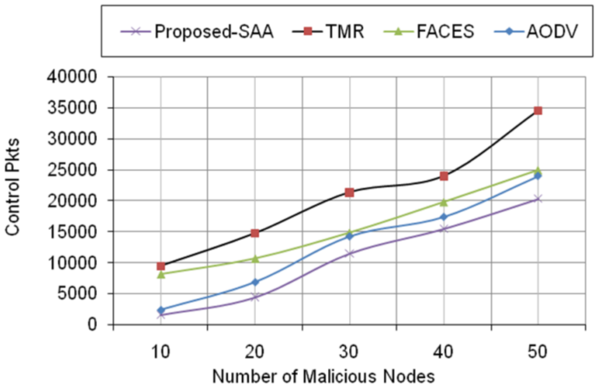

Fig.3. Control Overhead Comparison

- **End-to-End Delay:** It is calculated in expressions of average time taken for data packets for simulation. In Fig.4, the E-2-E delay of the protocol shows performance comparison. This explains the invariable rate of E-2-E delay for every protocol as an outcome of alterations in the number of harmful nodes. The SAA packets will be sent by a relatively low number of nodes to deliver packets with less delay. The presence of the overwhelming number of believable nodes, the delay may be delayed by a delay and a long way. In pertains to the performance of "reliability" and "trustworthy" nodes, the suggested SAA demonstrates a low E-2-E delay match up to with others, and in the situation of a high-fidelity node, it achieved a "99%" packet transfer with the lowest delay, as high trusted nodes utilized promptly too by the transmitter node to send data packets causing faster transmission rather than low trusted nodes.

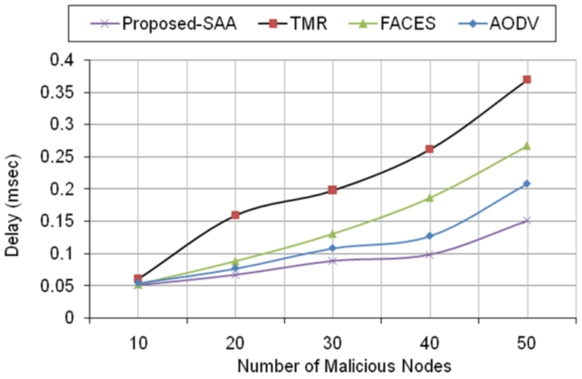

Fig.4. E-2-E Delay Comparison

V. CONCLUSION

In wireless MANET network security is considered as a measured challenge to manage due to its open channel and dependency on an intermediate node for the communication. In this paper, it suggested a self-assurance approach (SAA) relies on the trust mechanism to provide reliable and secure communication. The mechanism implements a probability assessment process to categorize the node behavior and predict its trustworthiness. It aims to solve the problem of the innocent node being punished due to other node's effects. Traditional approaches mostly compute the trust based on packet delivery and dropped or lost packets. In case of lost, it punishes all the nodes which affect all the node in route resulting in low performance. The mechanism SAA improve this

limitation through computing the probability model of isolation of node utilizing node conducts. The experiment investigation shows a satisfactory improvisation in comparison to other protocols in the variation of the count of MAL-Nodes. In the future, it will be explored against data privacy and its defense mechanism for further security enhancement.

REFERENCES

1. Z. Movahedi, F. Bayan, G. Pujolle, Z. Hosseini, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Adhoc Networks: A Survey", IEEE Comm. Surv. & Tut, Vol. 18(2), pp. 1287-1309, 2016.
2. K. Ullah, P. Das, A. Roy, R. Das "Trusted and secured routing in MANET: An improved approach", Int. J. of IEEE Symp. on Adv. Comp. and Comm., Pp. 297 - 302, 2015.
3. N. Marchang, S. K. Das, R. Datta "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Adhoc Networks", IEEE Tran. on Veh. Tech., Vol. 66(2), pp. 1684-1695, 2017.
4. S. A. Thorat, P. J. Kulkarni, "Design issues in trust-based routing for MANET", In Proc. of Intl. Conf. on IEEE Comp., Comm. and Netw. Tech., 2014.
5. M. Li, S. Salinas, X. Huang, J. Sun, and P. Li, "MAC-Layer Selfish Misbehaviour in IEEE 802.11 Adhoc Networks: Detection and Defence", Int. Jr. of IEEE Trans. on Mob. Comp., Vol. 14, 2015.
6. T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE Trans. on Mob. Comp., Vol. 14(4), 2015.
7. G. Zhan, Shi W, Deng J, "Design and Implementation of TARF: A trust-aware routing framework for WSNs", IEEE Trans. on Dependable and Secure Comp., Vol. 9(2), Pp. 184-197, 2012.
8. P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang, "Security in mobile ad-hoc networks using soft encryption and trust-based multipath routing", Int. Journal of Sci. Direct Comp. Comm., Vol. 31, 2008.
9. Chen, S. Garg, and K. S. Trivedi, "Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks", In Proc. of Intl. Workshop on ACM Modelling, Analysis, and Simulation of Wireless and Mob. Sys., Pp. 61-68, 2002.
10. Ahmed, K. A. Bakar, M. Ibrahim Channa, K. Haseeb, A. W. Khan, "A Survey on Trust-Based Detection and Isolation of Malicious Nodes In Ad-Hoc and Sensor Networks", Intl. Journal of Frontiers of Com. Sci., Vol. 9, pp 280-296, 2015.
11. J. Chang and S. L. Kuo, "Markov chain trust model for trust value analysis and key management in distributed multicast MANETs", IEEE Trans. Veh. Tech., Vol. 58, Pp. 1846-1863, 2009.
12. Xi, S. Liang, MA. Jian Feng, MA Zhuo, "A Trust Management Scheme Based on Behaviour Feedback for Opportunistic Networks", Intl. Journal of China Comm., Vol. 12(4), Pp. 117-129, 2015.
13. P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", Int. Conf. 6th Joint Working Comm. Multi. Security, Pp.107-121, 2002.
14. C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, Jul. 2003.
15. J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length", Int. Jr. of Netw. Comp. App., Vol.34, Pp. 1138-1149, 2011.

Retrieval Number: F4380049620/2020©BEIESP
DOI: 10.35940/ijitee.F4380.049620

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

16. N. Marchang, R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks", Intl. Journal of IET Info. Security, Vol. 6(2), pp. 77-83, 2012.
17. Z. Wei, H. Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning", IEEE Tran. on Vehic. Tech., Vol. 63(9), 2014.
18. Z. Wei, H. Tang, F. Richard Yu, M. Wang, and P. Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning", IEEE Tran. on Veh. Tech., Vol. 63, 2014.
19. G. Karame, I. Christou, and T. Dimitriou, "A secure hybrid reputation management system for super-peer networks", In Proc. of Int. Conf. on 5th IEEE Consumer Comm. Netw., pp. 495-499, 2008.
20. K. Paul and D. Westhoff, "Context-aware detection of selfish nodes in DSR based ad-hoc networks", In Proc. of Intl. Conf. on IEEE Global Telec, Vol. 1, Pp. 178-182, 2002.
21. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks", In Proc. of Intl. Conf. on ACM Mob. Comm., Pp. 255-265, 2000.
22. X. Mao and J. McNair, "Effect of on/off misbehavior on overhearing based cooperation scheme for MANET", In Proc. of Intl. Conf. on Military Comm., Pp. 1086-109, 2010.
23. T. Zahariadis, P. Trakadas, HC. Leligou, S. Maniatis , P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks", Int. Jr. of Wireless personal Comm., Vol. 69(2), Pp. 805-826, 2013.
24. T. Jenitha, P. Jayashree, "Distributed Trust Node Selection for Secure Group Communication in MANET", In Proc. of Intl. Conf. on IEEE 4th Advances in Comp. and Comm., 2014.
25. J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management Sys. for wireless sensor networks: Best practices", Intl. Journal of Comp. Comm., Vol. 33, Pp. 1086-1093, 2010.
26. R. Venkataraman, M. Pushpalatha, T. Rama Rao, "Regression-based trust model for mobile ad hoc networks", Intl. Journal of IET Info. Security, Vol. 6(3, pp. 131 - 140, 2012.
27. W. Li, A. Joshi, T. Finin, "Smart: An SVM-based misbehavior detection and trust management framework for mobile ad hoc networks", In Proc. of Int. Conf. on Military Comm., Pp. 1102-1107, 2010.
28. S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Sys.", IEEE Sys., Vol. 5, 2011.
29. S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol", In Proc. of Intl. Conf. on 6th Annual Symposium on Mob. Ad Hoc Network Comp., Pp. 226-236, 2002.
30. Y. Chae, "Redeemable reputation based secure routing protocol for wireless sensor networks", Master of Sci. Depart. Comp., Univ. Rhode Island, Tech. Rep. TR12-331, 2012.
31. Josang and R. Ismail, "The beta reputation system", In Proc. of Intl. Conf. on 15th Bled Electronic Comm., Pp. 41-55, 2002.
32. K. Paul, R.R. Choudhury, and S. Bandyopadhyay, "Survivability Analysis of Ad Hoc Wireless Network Architecture", Intl. Journal of Mob. and Wireless Comm. Networks, Vol. 1818, pp 31-46, 2000.
33. S. Abuhaiba and H. B. Hubboub, "Reinforcement swap attack against directed diffusion in wireless sensor networks", Intl. Journal of Comp. Netw. Info. Security, Vol. 5, Pp. 13-24, 2013.

AUTHORS PROFILE

Mr. T.Shekar Reddy (Tummala Shekar Reddy) Working as Assistant Professor in Department Computer Science at University College for women(A), Osmania University. He Obtained his Bachelor Degree in Computer Science and Engineering From AMIETE, New Delhi. He Master degree in Computer Science and Engineering from Osmanina University, Hyderabad. He has over 15 years of Experience in teaching. He area of Interests include Mobile Ad-hoc Networks, Wireless Sensor Networks, Network Security.

Mrs. Dr.Y.RamaDevi, Professor in Department of Computer science and Engineering ,CBIT(A). she has done Ph.D in Computer Science and Engineering from Central University of Hyderabad. She has done Head Dept .Of CSE and BOS in CBIT(A). She has Over 25 years teaching and Guidance to U.G & P.G and Research Scholar. She area of Interests Include Mobile Ad-hoc Networks ,Data Mining ,Bio-Informatics.