Security Improvisation through Node Trust Prediction Approach in Mobile Ad Hoc Network

https://doi.org/10.3991/ijim.v13i09.9329

Raghavendar Raju L(✉)
Matrusri Engineering College, Telangana, India
lraghavenderraju@gmail.com

C R K Reddy
Mahatma Gandhi Institute of Technology, Telanagan, India

Abstract—Identifying trusted nodes for safe communication is a key challenge in mobile ad-hoc networks. Node compromises a service and leads to uncertainty in node behaviour. Computing the node trust and node management will enhance the security aspect in MANETs. This paper proposes a security improvisation based on a Node Trust Prediction Approach (NTPA). NTPA aims to prevent the interference of an anomalous node in a MANET. There by improving the ***security and data delivery output***. The NTPA calculates the node trust prediction by evaluating the four most frequent actions that are performed by a node in the communication process. *Node authorization* is a key aspect in the evaluation of an ad hoc network's security. In the proposed method, we monitor the *valid* and *Invalid Authorization* of a node. Data delivery reliability is measured with S*uccess of Packet delivery* and *Loss or Drop of packets.* In this paper, NTPA is compared with SAR (Security-Aware Routing) and AODV (Ad hoc on-Demand Distance Vector), to evaluate the efficiency in an ad hoc network. The empirical results show that there is an increase of 25% packet delivery and a 40% reduction in routing overhead.

Keywords—Security, Trust Computation, Node Trust Prediction, MANET.

1 Introduction

A mobile ad-hoc network (MANET) is a network having a number of wireless devices that are proficient in interacting with each other. Due to dynamic environment, sharing of channels and computation constraints, MANETs are more vulnerable to security attacks compared to traditional wireless networks. For a possible multi-hop communication among non-adjacent nodes, former nodes must function as routers. This constraint poses a great challenge to find a reliable node that acts as a router for secure communication in MANETs.

To accomplish benchmark performance in reliable communication, the routing technique must be adaptable to dynamic environmental format. The mobility of the nodes can result in loss of existing links. Hence there is a need to discover new paths to overcome the communication disruption. The presence of faulty nodes hinders ad hoc networks through entering "incorrect routing updates", "responding to out dated routing information", "changing routing updates or advertising false routing information" and "dynamic characteristics of ad hoc networks" [4], [9], [11], [12]. Many frameworks [1], [2] and methods [5], [7], [3] are available in relational and reliable computational-based security models that are more effective for limited resource communication.

The mechanism of routing in MANET relies entirely on the coordination and participation of neighbourhood nodes [11]. A misbehaving node causes data loss and imbalances the network. A powerful, steady and secure routing protocol is required to achieve quality, secure performance standards, effective maintenance of the node-link and mobility of a MANET.

The trust system will keep the available network services in safe state. For instance, "quality assessment", "access control", "authentication", "malicious node detection", and "secure resource sharing" of information received [3], [6], [8], [9], [13]. As a result, it is significant to regularly estimate the trust values of nodes based on certain metrics and calculations. In this paper, we propose the **Node Trust Predicting Approach (NTPA**) to recognize the Node Trust. It is used to establish more secure communication on Mobile Ad hoc Networks. Many strategies related to trust computation [15], [16], [17] have been proposed in these networks. In the proposed methodology, a comprehensive node trust prediction based on "Valid and Invalid Authorization", and "data routing actions" have been carried out to improve the security of MANET by increasing node-level trust characters.

The remaining paper is structured as follows. Section 2 discusses correlated research on trust-based routing and security enhancement. The proposed Node Trust Prediction Approach (NTPA) mechanism is discussed in Section-3. Section-4 explains the experiment and outcome assessment, followed by conclusions in Section-5.

2 Related Work

Network to establish trust management mechanism, effectively improves network security [1], [2]. Trust has been noticed in several areas of security systems and has become more and more important in wireless networks [4], [10]. Each security document method has its own subject qualification and filtering issues. Trust-based security techniques are important in MANET-based approaches and have been studied in numerous recent literatures [18], [19], [20]. The rich literature surrounding trust and its management in the network makes us strongly suggest that this is an important and exciting area of research. The trust has an extensive diversity of alterations and functions as a concept that leads to disagreement over trust management terminology. And while prevention-based approaches prevent inappropriate behavior, malicious nodes still have the opportunity to contribute to the routing process and disrupt appropriate routing concern. Commencing the familiarity of wireless network security design and the multi-level security mechanism it is highly required for future secure communication.

K. Govindan et al. [3] conducted a detailed investigation of various trusted computing methods for MANET. It provides MANET designers multiple viewpoints on the impression of trust, a considerate of the attributes that have to be well thought-out in extending trust metrics, and within reach on how to calculate trust. It suggests an all-inclusive assessment of a variety of trust calculation methods, as well as comparisons of diverse "attack models" and "computational prerequisites". It also analyzes diverse documents of "trust dynamics", such as "trust propagation", "aggregation" and "forecasting".

Z. Wei *et al.* [5] projected a" trust management scheme". The trust model has two components: "direct surveillance of trust" and "indirect surveillance of trust". Direct surveillance from the observer node, the trust value is derived using "Bayesian presumption", which is an uncertainty assumption, whilst the complete "probability model" be able to be characterized. On the other side, indirectly observing second-hand information about neighbor nodes, also called observer nodes, using DST (Dempster-Shafer theory) to derive trust values, DST is another type of uncertainty inference that can be derived indirectly. By uniting these two constituents in the trust model, a further perfect trust value for observing nodes in MANETs can be obtained.

A. Pirzada *et al.* [21] proposed routing-based direct trust computing. It describes the trust as a fractional value in [x0, 1] and assesses the performance of the AODV and DSR protocols and analyzes it with the proposed trust scheme. In this scenario, nodes always monitor neighbors to build and update trust relationships. Sun et al. Consider the uncertainty of trust as being properly implemented by observed nodes, using entropy to develop a trust model, and assessing trust values through straight surveillance. The "Indirect or indirect information" possibly imperative in assessing the trust of observing nodes as compared to direct observations in confidence assessments. For illustration, a set of proofs as of neighboring nodes be able to identify that a malicious node achieves a good situation for one observer instead of another.

A routing protocol based on "Security-Aware Routing (SAR)" [22] mechanism transforms the "AODV routing protocol" [14] to comprise the trust hierarchy of integration nodes for path assessment and assortment. The protocol executes the trust level in terms of to the organization level and uses the "shared key" of every one layer in order to facilitate nodes be able to specify security prerequisites whilst apply for routes. Merely nodes that assemble this necessity can contribute to the routing. But how to classify "node trust", "key distribution" and other key awareness of nodes is a significant scope of the current research works.

Predicting node trust dynamics means that node trust should change according to its behavior. Non-transitive means that "Node-A does not unavoidably trust Node-C if Node-A trusts Node-B and Node-B trust Node-C". In asymmetry, it means that "Node-B does not essentially trust Node-A if Node-A trusts Node-B". Perspective dependent resources that trust estimation is usually derived from the behavior of nodes. The dissimilar phase of action can be accessed through dissimilar trusts. For instance, if a node consumes a smaller amount of power than it could not be capable of self-assured the message to its neighbors. In such case, the energy trust of this node will decrease, however, the "security trust" of this node determination not change because of the status. To calculate the level of trust on a node, it is important to understand the various trust features used for trust definitions, metrics, and trust calculations. The trust of a meticulous node is a prejudiced consideration of the reliability and accuracy of the information the node's agent receives or passes through in that given context. The MANET routing protocol is used to evaluate the proposed protocol for SAR [22]. The following sections define the process of distributing trust keys and trust calculation and routing mechanisms.

3 Proposed Node Trust Prediction Approach

The proposed Node Trust Prediction Approach (NTPA) is shown in Fig.1. It is a three-step process. First step involves, a node to secure itself in a given network (A in Fig1). To secure itself, it acquires a Trust Certificate from Certified Authority (CA), which consists of a "Public Key as CA_{pub_key}" and "Private Key as CA_{pvt_key}". Based on these authorized keys it authenticates the node during data routing. In the second step (B in Fig1), it performs the Node Trust prediction and finally(C in Fig1) based on individual trust prediction of a node, it performs a secure trust-based routing.

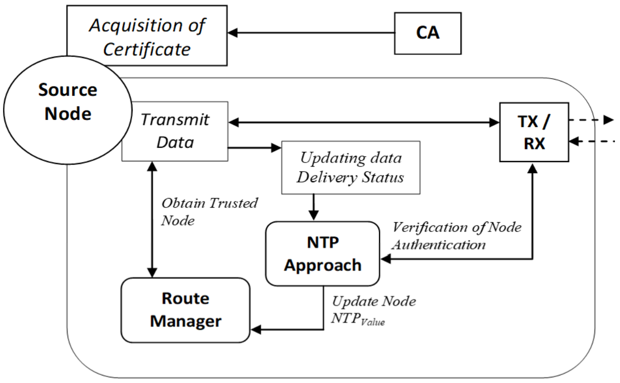
Acquisition of Certificate
CA
Source Node
Transmit Data
TX / RX
Updating data Delivery Status
Obtain Trusted Node
NTP Approach
Verification of Node Authentication
Route Manager
Update Node NTP_{Value}

Fig. 1. Proposed NTP Approach Architecture

3.1 Acquisition of trusted certificate

Before joining the network, every node in the network has to acquire a secure "trust certificate" from a "trusted certification authority (CA)". Security certificates that have been released cannot be "Withdrawn or expired"untilanode exists in the network. If the node's trust value drops below the 40%threshold, the certificate will be invalidated. This means that the legitimacy of the certificate determination is maintained until the credibility is preserved. In such progression, NTPA is capable of recognizing nodes that have illegitimately own a valid certificate and avoid the intrusion of malicious nodes in the routing process. The certificate issued by CA is denoted as CA_{cert}.

$$CA_{cert} = E(ND_{add}, ND_{pu\,b_{key}}, CA_{pu\,b_{key}}, E(NTA_{key})_{ND_{pv\,t_{key}}})_{CA_{pvt\_key}}$$

Where,
E - Encryption
CA_{pub_key} - Public Key issued by Certified Authority.
CA_{pvt_key} - Private Key issued by Certified Authority.
NTA_{key} - Node Trust Authentication Key.
ND_{add} - Node Address.
ND_{pub_key} - Node Public Key.
ND_{pvt_key} - Node Private Key.

Each node is preloaded with this CA_{cert} certificate before joining the network and it produces NTA_{key}in case of authentication verification. The acquired authentication acts as an attestation for a node, thus making it a valid node in the network.

3.2 Node trust prediction computation

The evidence of a node trust was computed utilizing the three monitoring factors of a node: authentication, data delivery, and data loss. The process of authentication involves a node to produce its CA authentication key NTA_{key} to recognize it as valid A_{valid}andinvalid authorization as $A_{invalid}$. Similarly, the process of data delivery as R_{data} and loss as $L_{data}$is measured based on the acknowledgement being received by the destination or intermediate nodes. $A_{valid}/A_{invalid}$ and R_{data}/L_{data} are utilized for computing the node trust prediction value as NTP_{value} of a node.

Each of these values is recorded on each data packet being transmitted through the participating intermediate nodes. The positive outcome of authorization A_{valid} and successful delivery of data packets R_{data} increases a node credit by 1 and at the same time its debited by 1 in case of invalid authorization $A_{invalid}$ and in case of data delivery fail or loss L_{data} is increased by 1. Each of these parameters can be illustrated as:

Valid Authentication	$A_{valid} = A_{valid} + 1$
Invalid Authentication	$A_{valid} = A_{valid} - 1$
Data Delivered Success	$R_{data} = R_{data} + 1$
Data Delivered Failed	$L_{data} = L_{data} + 1$
Data Loss	$L_{data} = L_{data} + 1$

On the basis of the values of A_{valid}, $A_{invalid}$, $R_{data,}$ and L_{data} , we compute each individual node's rate of authorization as $A_{rate}$and rate of data delivery as R_{rate}. The percentage of this rate can be computed using the Eq.1, Eq.2 and Eq.3 as given.

$$A_{rate} = \frac{\sum A_{valid}}{n} \times 100 \tag{1}$$

$$R_{rate} = \frac{\sum R_{data}}{d} \times 100 \qquad (2)$$

$$L_{rate} = \frac{\sum L_{data}}{d} \times 100 \qquad (3)$$

$$NTP_{Value} = \frac{(A_{rate} + R_{rate}) - L_{rate}}{2} \qquad (4)$$

Based on A_{rate}, R_{rate}, and Lrate values, we compute the NTPvalue using the Eq. 4. The NTPvalue is utilized for the runtime trusted node selection to route data from the source node to the destination. The NTP_{value} used as the value limit for a node's consideration for communication and this node is used as a source node.In the next section, we discuss the trust prediction routing mechanism based on NTP_{value}.

3.3 Trust prediction-based routing

The main objective of routing methods in the Adhoc network is to provide efficient data routing. Each node in the proposed protocol sends data through the discovered path and predicting each node's NTP_{value}. The protocol presupposes that the entire nodes on the network are, to begin with, reliable and trustworthy. The "trust value" is computed based on the value of this NTP_{value} derived using the Eq. 4.

The source sends data packets to the destination through the cached route by the route manager. Initially, all nodes NTP_{value} is considered as 100%. To begin with, source selects the shortest hoping path. During routing each node asks its neighbour nodes to produce a CA_{cert} certificate to get authenticated before transmitting the data packet. In case of success it updates A_{valid} and $A_{invalid.}$. Similarly it updates it R_{data} and L_{data} in case of successful data delivery or failure. On continuous observation of these values it computes its A_{rate} , $R_{rate,}$ and L_{rate} values and finally it computes its NTP_{value} and updates the routing table. An illustration of node trust routing table is given in Table-1.

Table 1. Source Node Routing Table

S. No.	Route	Prev_Hop	First_ Hop	NTP_{value}
R1	6,3,4,2,D	S	6	38
R2	**4,5,3,8,10,D**	**S**	**4**	**68**
R3	6,3,8,5,12,D	S	6	60
R4	3,7,8,2,9,D	S	3	35
R5	3,6,5,11,9,12,D	S	3	35

For example, in Table-1, it shows 5 routes to destinations and each route 1st hop and NTP_{value}, the most efficient and shortest route is R1, but as per the NTP_{value} derived using the equation (4), the route R2 1st hop is more trustful in compare to route R1. So, it is viable to route data through R2 instead of R1. The process of selection of node and routing is available in Algorithm-1.

Algorithm 1: Data Routing Based on the Node Trust Prediction.

```
Data Transmission initialization by Source Node, S.
TransmitData ($S_{add}$,,$D_{add}$ , Data, seq_no);
// $S_{add}$: Source address, $D_{add}$ : Destination address, seq_no: sequence Number
Method: transmitData ($S_{add}$,,$D_{add}$ , Data, seq_no)
// Threshold of $NTP_{value}$
Th_NTP = 40%;
// Read First Hop Nodes from Routing Table
FH_N[x] = getFirstHop_Nodes();
P = Number of data packets to transmit.
H = sizeOf (FH_N[x]);
// Loop until Number of data packets to send
For (d=0, d<P, n++) Loop
    For (h=0, h<H, h++) Loop
        FH = FH_N [x,h];
        $NTP_{value}$ = getNodeAuthentic_Rate(FH);
        If $NTP_{value}$ >= Th_NTP Then
            TransmitData($S_{add}$ , $D_{add}$ , Data, seq_no);
        else
            check for Next available Hop $NTP_{value}$ ;
        end If;
    End For;
End For
```

The "intermediate nodes" also go after the identical plan as the "original source node" function. Table-2 illustrates the node's routing table for "Node-4" which has two hopes. According to this table input and its first_hop NTP_{value} it selects the route R1 node as its NTP_{value} value is higher in comparison to R2 node.

Table 2. Routing Table for Node-4 as Intermediate Node

S.No.	Route	Prev_Hop	First_ Hop	NTP_{value}
R1	6,3,**4**,**2**,D	4	2	**65**
R2	**4**,**5**,3,8,10,D	4	5	50

The source node performs a list of "sequential numbers of packets" sent by it. On arrival of successful acknowledgment, source updates the R_{data} of each node in the route. In case of packet loss, it punishes a node by decreasing the R_{data} value. This dynamic routing based on the runtime NTP_{value}(derived from equation (4))provide a reliable and secure routing. Also assures a confirmed delivery in case of arbitrary selection of a node or predefined route nodes.

4 Empirical Assessment

4.1 Simulation set-up

Experiment simulation is performed using Glomosim Simulator, we have modified the "AODV protocol" to evaluate the "NTPA protocol", and evaluate the effectiveness of our projected protocol with "SAR" [28] and "AODV" [16]. As we added security parameters, the route request and the size of the routing's packet header are increased. We configure the simulation by means of the subsequent setup constraints as illustrated in Table-3.

We execute the experimentation based on the Table-3 simulation factor for a time of "600 seconds" with an RWP movement behavior model with varying speeds between "0 to 100 m/s". We execute the simulation in six dissimilar speed as configured in Table-3. For data routing, we used "15 source-target pairs" of "constant bitrate (CBR)" traffic of "4 packets per second", and each "512 bytes" in size. The assessment was conducted in two different situations. First, there were not any misbehaving nodes in the network, followed by 25% of the misbehaving nodes added. The experimental outcomes demonstrate the "overhead introduced" caused by security enhancements and "throughput" comparisons.

All nodes behave normally during route discovery. However, 25% misbehaving nodes are randomly selected by route simulator. Nodes will behave abnormally discarding all data packets and generating incorrect trust prediction. However, using signature verification in NTPA can detect any type of packet modification attack. Packet drops can isolate abnormal nodes from the network. For performance assessment, we determined the following "throughput" and "control overhead" metrics.

Table 3. Simulation Parameters

Configuration	Parameter Values
Simulation Dimension	“1000X1000”
Distributed Nodes	“50”
RWP Mobility	“0 to 20 m/s”
Source-Target pairs	“15”
Size of Pkts in Bytes	“512”
Rate of packet Transmission	“4 pkts/sec”
Variation of Mobility (m/s)	“0, 20, 40, 60, 80, 100”

4.2 Result analysis

Throughput: Throughput is determined to utilize the "Total Number of Delivered" by "Total Number of Packets Send". To provide performance comparison analysis for a better insight of our simulation results shown in Fig.3 and 4 show the throughput outcome of the protocol. In the absence of malicious nodes, all protocols show similar results. Compared with the AODV and SAR protocols that have malicious nodes, NTPA shows improvement. Increase in the throughput is due to secure data routing by the trusted nodes. In the nonexistence of malice, it shows an average outcome as a result of security overhead. NTPA achieved a 25% improved packet transfer compared to other approaches, while others showed a 10-20% drop with 25% of malicious nodes presences in the network.

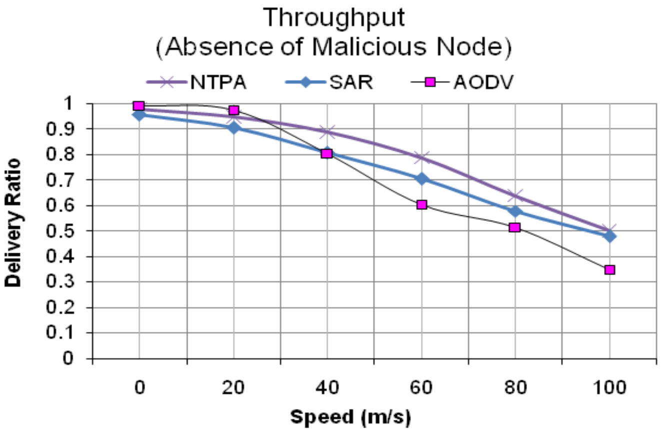

Fig. 2. Avg. Delivery ration in Absence of Malicious Nodes

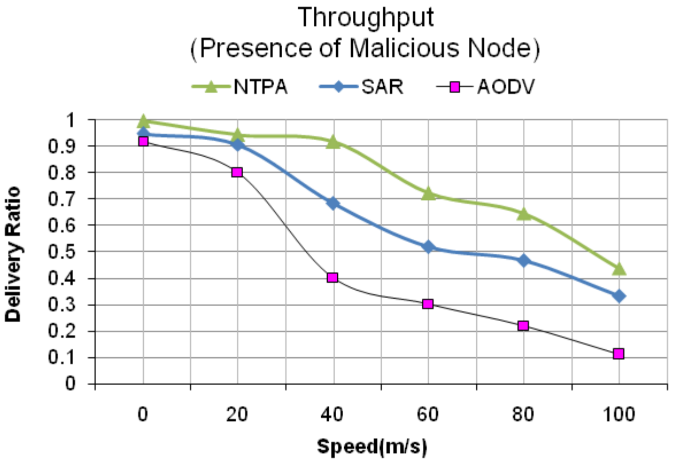

Fig. 3. Avg. Delivery ratio in Presence of Malicious Nodes

Control overhead: Control overhead determination is based on the "total number of control packets originated and forwarded" by the approaches for the period of complete communication progression. To provide performance comparison analysis for a better insight of our simulation results shown in Fig.5 and 6show the control overhead between NTPA and other methods. In the "absence of malicious nodes", the entire protocols comprise a comparable overhead ratio.

However, in presence of malicious node NTPA shows lower routing overhead. Because NTPA uses trust prediction to identify misbehaving nodes and discards them to minimize control packets. In SAR repeated security checks are perform during communication. In AODV, during speed changes high speed links will fail. Also malicious nodes add high control packet switching. This raises their routing overhead compare to NTPA.

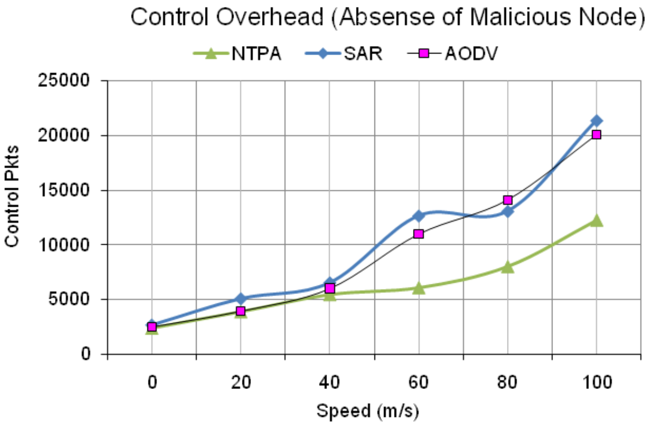

Fig. 4. Avg. Control Overhead in Absence of Malicious Nodes

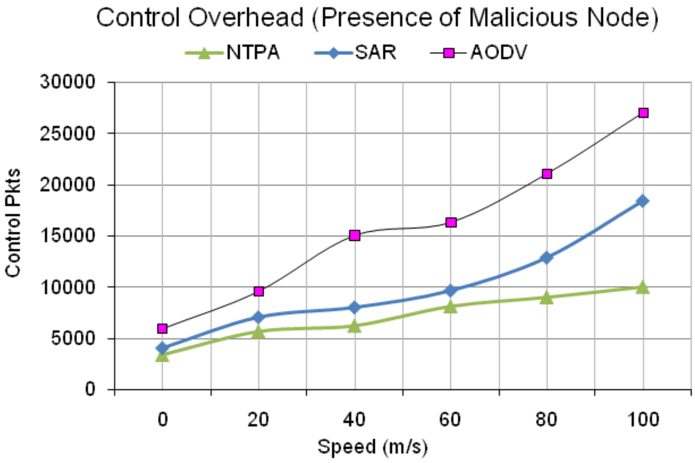

Fig. 5. Avg. Control Overhead in Presence of Malicious Nodes

We propose an innovative "Trust-based secure routing protocol", NTPA, for mobile ad hoc networks. NTPA authenticates the routing node based on the "trust certificate" and "trust prediction" computed during communication. NTPA supervises multiple routes to reach the target node. Each node in the network accumulates a "local trust value" of each other node and maintains the routing table. The NTPA calculate the trust value of all nodes in the first hop. Intermediate nodes, route, data packets by choosing a path with a higher value of trust nodes. The mechanism for security improvisation based on NTPA helps in improvising the throughput of PDR during communication. The empirical results show a 25% of high PDR with minimal overhead. In mutual cases, NTPA commences a practical network load to ascertain more packet transmission rates. This increase can result in shorter trust values and convergence time. In addition, more work needs to be done in the future to measure the effect of any change in protocol parameter values and to find the best value for different settings.

5 References

[1] Z. Movahedi, Z. Hosseini, F. Bayan, G. Pujolle, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey", International Journal of IEEE Communications Surveys & Tutorials, Vol. 18(2), Pp. 1287 - 1309, 2016. https://doi.org/10.1109/comst.2015.2496147

[2] K. Ullah, R. Das, P. Das, A. Roy, "Trusted and secured routing in MANET: An improved approach", IEEE International Journal of Symposium on Advanced Computing and Communication, Pp. 297 - 302, 2015. https://doi.org/10.1109/isacc.2015.7377359

[3] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, 2012. https://doi.org/10.1109/surv.2011.042711.00083

[4] J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks", IEEE Communications Surv. Tuts., Vol. 13, no. 4, pp. 562-583, 2011. https://doi.org/10.1109/surv.2011.092110.00088

[5] Z. Wei, Helen Tang, F. Richard Yu, Maoyu Wang and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning", IEEE Transactions on Vehicular Technology, Vol. 63, No. 9, November 2014. https://doi.org/10.1109/tvt.2014.2313865

[6] N. Marchang, R. Datta, S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks", International Journal of IEEE Transactions on Vehicular Technology, Vol. 66(2), Pp. 1684 - 1695, 2017. https://doi.org/10.1109/tvt.2016.2557808

[7] W. L. and M. Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Vol. 63, No. 9, Nov. 2014. https://doi.org/10.1109/tvt.2014.2313180

[8] T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", International Journal of IEEE Transactions on Mobile Computing, Vol. 14, No. 4, Apr. 2015. https://doi.org/10.1109/tmc.2014.2330818

[9] A. 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", International Journal of Frontiers of Computer Science, Vol. 9(2), pp. 280-296, 2015. https://doi.org/10.1007/s11704-014-4212-5

[10] J. Hassan, H. Sirisena, and B. Landfeldt, "Trust-based fast authentication for multi-owner wireless networks", IEEE Trans. Mobile Computer, Vol. 7, no. 2, pp. 247-261, 2008. https://doi.org/10.1109/tmc.2007.70720

[11] R. Changiz, H. Halabian, F. R. Yu, I. Lambadaris, and H. Tang, "Trust establishment in a cooperative wireless relaying networks", Wireless Communications Mobile Computer, Sep. 2012. https://doi.org/10.1002/wcm.2271

[12] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", In ACM/IEEE Int. Conf. on Mobile Computing and Networking (MOBICOM'2000), Feb. 2000. https://doi.org/10.1145/345910.345958

[13] L. Kagal, T. Finin, and A. Joshi, "Trust-based security in pervasive computing environments", IEEE Computer, Vol. 34, pp. 154-157, 2001. https://doi.org/10.1109/2.970591

[14] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF RFC 3561, Jul. 2003. https://doi.org/10.17487/rfc3561

[15] H. Sarvanko, M. Hyhty, M. Katz and F. Fitzek, "Distributed resources in wireless networks: Discovery and cooperative uses", In 4th ERCIM eMobility Workshop in conjunction, 2010.

[16] M. A. Ayachi, C. Bidan, T. Abbes and A. Bouhoula, "Misbehavior detection using implicit trust relations in the AODV routing protocol", In International Symposium on Trusted Computing and Communications, Trustcom, pp. 802-808, 2009. https://doi.org/10.1109/cse.2009.125

[17] A. Boukerch, L. Xu and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks", In Computer Communications, no. 30, pp. 2413-2427, 2007. https://doi.org/10.1016/j.comcom.2007.04.022

[18] S. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks", IEEE Trans. Veh. Technol., Vol. 60, no. 3, pp. 1025-1036, Mar. 2011. https://doi.org/10.1109/tvt.2010.2103098

[19] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks", in Proc. 2nd Workshop Economy. Peer-to-Peer System, pp. 1-6, 2004.

[20] J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length", International Journal of Network Computer Application, Vol.34, No.4, pp. 1138-1149, 2011. https://doi.org/10.1016/j.jnca.2010.11.007

[21] A. Pirzada and C. McDonald, "Trust establishment in pure ad-hoc networks", Wireless Personal Communications, Vol. 37(1-2), pp. 139- 168, 2006. https://doi.org/10.1007/s11277-006-1574-5

[22] S. Yi, P. Naldurg, and R. Kravets. Security-aware ad-hoc routing for wireless networks. In MobiHOC Poster Session, 2001. https://doi.org/10.1145/501449.501464

6 Authors

Raghavendar Raju L is from Matrusri Engineering College, Telangana, India. lraghavenderraju@gmail.com

C R K Reddy is from Mahatma Gandhi Institute of Technology, Telanagan, India.

Article submitted 2018-08-02. Resubmitted 2019-06-11. Final acceptance 2019-06-12. Final version published as submitted by the authors.