Indian Journal of Science and Technology, *Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/98497, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Secure Data Transmission in Integrated Internet MANETs Based on Effective Trusted Knowledge Algorithm

C. Atheeq and M. Munir Ahamed Rabbani

B. S. Abdur Rahman University, Seethakathi Estate, Vandalur, Chennai – 600048, Tamil Nadu, India;
atheeq.prof@gmail.com, marabbani@bsauniv.ac.in

Abstract

The communication between mobile node and fixed node is achieved through the Integrated Internet MANET (IIM) with the help of the gateway by increasing the application domain of mobile ad hoc network. The wireless channel and dynamic nature of Mobile Ad hoc Networks (MANETs) experiences integrated MANETs to suffer from security susceptibility. **Methods/Analysis:** An untrustworthy mobile node can harm the data and adversely affect the communication between a mobile node and a fixed node in IIM. In this manner, examining the trust level impacts the certainty with which an element may decide for information transmission. In order to provide a secure data transmission we are proposing an Effective Trusted Knowledge Algorithm (ETKA) that calculates the nodes trust. **Findings:** The proposed algorithm has two phases for finding the trusted node. In the first phase, observing the nodes in promiscuous mode, in the second phase, the effective trust value is calculated by hybrid method. **Improvement:** Through extensive simulation analysis, we can come to an end that the developed mechanism leads to a successful methodology towards security and protection of data from untrusted nodes in integrated internet and MANET.

Keywords: Integrated Internet MANET, Promiscuous Mode, Trusted Table, Trust Value

1. Introduction

An Infrastructure less wireless network is termed as MANETs[1]. A MANET is collection of several nodes that send and receive data directly in a peer-to-peer method. Thus, a specially appointed system is autonomous of any current system foundation, for example, base stations and access points. In spite of the fact that a self-ruling, MANET is helpful as a rule, a MANET associated with the Internet is considerably more alluring. This is on the grounds that Internet assumes a critical part in the day by day life of many individuals by offering an expansive scope of administrations. Gateways are used to integrate the wireless mobile ad hoc network and the wired cyber-space and ad hoc routing protocol that is required to send packets from MANET to internet as well as within a MANET. The integrated internet and MANET is represented in Figure 1.

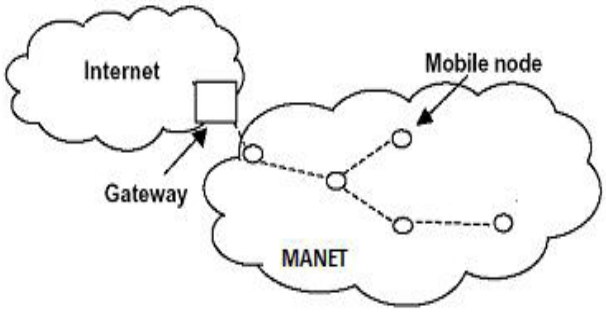

Figure 1. Integration of internet and MANET.

**Author for correspondence*

The ad hoc routing protocols proposed for MANETs which are used to communicate information among freely moving communicating entities. Mobile devices communicate with one another using multi-hop relaying[2]. But, it is not possible for the mobile nodes to access internet because routing from static node and a mobile node is not supported. In the I-D "Global Connectivity for IPv6 Mobile Ad Hoc Networks"[3] an answer is displayed where Ad hoc on-demand distance vector is altered in a manner that it can route packets both in integrated network and MANET, but it is not considering security mechanism.

The main challenge here stems from the need of selecting a trusted mobile node in MANET for secure data transmission in the field of integrating internet with MANET. So, an effective trusted mechanism is needed for this environment in such occurrence; the mobile node has to choose which of its neighbor trustworthy node the optimal one for its communication is, Examining and labeling the different security issues in the way connected from a MN to the FN, by checking the behavior of the suspicious nodes in the composite network frames the inspiration of the research[4].

There might be untrusted nodes or congested nodes present in MANET which drops the packets in the path to the fixed node. The existence of untrusted nodes may not be known to the source node. These reasons made us to build up a trust based system that recognizes these mischievous activities of the nodes in the MANET furthermore guarantees choice of trustworthy nodes[4]. Trust framework can likewise be utilized as a part of evaluating the nature of received information, to give network security administrations for example access control, authentication, identifying untrusted node and secure asset sharing[5-8]. Therefore, it is vital to occasionally assess the trust estimation of nodes in view of a few measurements and computational strategies. Trust calculations in static systems are generally less difficult in light of the fact that the trust value here changes for the most part because of conduct of nodes. Sufficiently after perceptions these practices are unsurprising.

In order to have an effective trust on the nodes, we are proposing ETKA that detects the nearness of suspicious node and protect the data being transmitted from them. It basically does the work in three different stages. Initially each node in a system follows to its adjacent nodes randomly for observing the behavior of the nodes and the misbehaving nodes are considered to be malicious from the remaining nodes it assigns a task for the mobile nodes and the nodes that are providing inappropriate results or delays the task completing time then such type of nodes are treated as unfair nodes and in the final stage from the remaining nodes effective trust is calculated by hybrid method.

The remaining part of the work is arranged as follows. Section II illustrate related work for security issues in the integration of internet and MANET, section III tell of the proposed work and section IV Analyses the simulation outcomes and section V concludes the paper.

2. Related Work

In the survey, lot of strategies have been worked out for inter connecting internet with MANET and the techniques used for calculation and management of trust and the security measures considered. Gateway discovery is done by the three approaches namely reactive, proactive and hybrid by extending Ad hoc On-Demand Distance Vector (AODV) routing protocol that are addressed by Ali Hamedian et al.[9], very few papers focused on secure data transmission between fixed node in internet and a mobile node in MANET.

Sanjay et al.[10] have proposed a strong method to bear the cost of security for MANETs and performs superior to the trust depended mechanisms through it has been analyzed. The friends sharing method ends up being a proficient instrument to open out data of trustworthy nodes adequately in framework. Faultiness of a node is on the solitary circumspection of a specific node that decides from tasks. In their protocol, they have used difficulties besides other secure protocol which uses multi hop routing & records the neighbors work to verify any node contrasted and because of these difficulties, the FACES mechanisms works more preferable & gives much security over the other multi hop routing protocol. If we increase the application domain of MANET by interconnecting with internet then the security parameters should be considered for the connectivity in order to have the efficient data communication between the mobile nodes and the internet resources.

Ayesha, Sridevi and Arshad11 have proposed an algorithm for moderating black hole attack in AODV protocol based on secure knowledge. It focuses the packets which are sent in promiscuous mode to guarantee that the packets are conveyed to its destiny before concluding that a particular node is black hole node, our algorithm monitors the node for packet

drop reason, in this way keeping a trusted node from turning into a black hole node. But to have effectiveness of the data transmission, authentication of the nodes is also required where we can conclude that the data is being transmitted through trusted nodes in a secure route.

Amit kumar et al.[12] Gupta has provided a method in which trusted secure gateway is selected and authenticating it so as to achieve host to host security by means of trusted and uncongested route and trusted node. However this concept is limited in MANETs i.e. only communication is provided only between mobile nodes of MANET, a fixed node from Local Area Network (LAN) or internet is not possible to communicate in this scenario.

Antesar M. Shabut et al.[13] have proposed a suggestion based trust system with a protection plan, which uses clustering strategy to progressively removing attacks identified with exploitative proposals between certain time in light of number of connections, similarity of data and closeness between the nodes. In IIM, as the gateway is used for connectivity, the recommendation based trust model may not provide better security as the nodes behave irresponsible.

Chen Xi, Sun Liang, Ma Jianfeng and Ma Zhuo[14] have represented a new scheme for trust management based on behavior feedback in which the fast-moving nodes realize the mutual identity authentication by utilizing the certificate chains, and the identity trust relationship is built up in certificate graph format. On the other hand, the successors generate Verified Feedback Packets for each positive feedback behavior to realize the mutual authentication of forwarding behavior, and consequently the behavior trust relationship is formed. The studies can be implemented in Internet MANET Integration for the mobile nodes to have better resource utilization in order to provide secure data transmission.

Yichi Zhang, Lingfeng Wang and Weiqing Sun[15] concentrated on the essential parts of the trust framework arrangement that are static trust node situation, dynamic ideal communication between a routing algorithm which is fault tolerant and cost-delicate and they chose nodes. A three-layer conveyed interruption discovery framework design proposed in[16] is utilized as the trust framework to be sent in the smart grid network; specifically, it is utilized to find the trust nodes and actualize the optimal routings. As the nodes in MANETS are dynamic in nature it would not provide the placement of the node and ideal conversation between fixed node and mobile node in IIM is achieved through the authentication system based on trust values.

Wang et al.[17] proposed a method to recognize childish nodes from agreeable ones construct exclusively in light of nearby perceptions of AODV routing protocol practices. They utilize a confined state machine structure of privately watched AODV activities to build a measurable portrayal of every nodes conduct. With a specific end goal to recognize selfish and cooperative nodes, a progression of surely understood measurable tests are connected to highlights acquired from the watched AODV activities. An intriguing expansion of this work is considered for different examples of node mobility which can give extra bits of knowledge.

In the above survey, most of the proposed models (10, 11, 12, 13, 15, 17) are based on trust evaluation of the nodes and routes for providing security and identifying malicious nodes and protecting the data from unauthorized user and these papers are limited to only MANET region but to provide effective communication, mobile nodes have to utilize the internet resources. So our proposed model increases the application domain of MANET by interconnecting with internet. In paper[14], the security measures based on certifications and key management techniques has been worked out. But if we enhance the secure data transmission by also considering the trust evaluation scheme for node selection and data transmission will filter out the malicious nodes effectively.

So in this paper, we are first filtering out the malicious nodes from the network through promiscuous mode and then for the remained trusted nodes, we are finding the trust values based on the hybrid methods and the mobile node that is having the maximal trust value is chosen for data transmission. In this way we are providing effective security for the data that is being transmitted in IIM

3. Proposed System

We propose an ETKA for secure routing amid mobile node in MANETs and a fixed node in internet. The proposed model is split in to two aspects one is for selecting of trusted node from the network using promiscuous mode and the other is for evaluation of effective trust value using hybrid method. The architecture of IIM with the presence of pernicious nodes and the trusted nodes is represented in Figure 2.

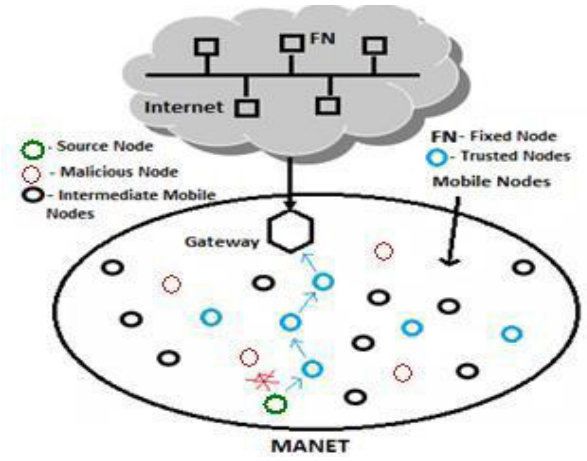

Figure 2. Presence of pernicious nodes and trusted nodes in IIM.

3.1 Phase 1: Selection of Trusted Nodes

In this phase, each mobile node watches its neighbor nodes in promiscuous mode that the packet are being sent by its neighbors with a specific end goal to record the conduct of neighbor in regards to packet operation in the trusted knowledge table that is kept up by each node. Each mobile node contrasts the neighbor data and the data it records in its trusted knowledge table. In the event that both are same, they are named as trusted nodes which expect that the packet is sent further, else it waits for specific time period and checks the purposes behind packet dropping. When packet dropping reaches the threshold value, then the nodes are declared malicious nodes. It is then recorded in the field M_ip_addr of trusted knowledge table and a message is broadcasted in the network announcing that the particular node is malicious and it can be refrained in the routing. Keeping in mind the end goal to affirm, the packets are delivered to its adjacent nodes, the trusted nodes screens all the packets to refrain from selective dropping, as the selected packets are dropped by untrusted nodes. Our algorithm is built on AODV routing protocol, but it can be only used in MANETs. So in order to support routing process in integrated internet MANET, modified AODV (MAODV)[19] is used where the best path is built on smallest hop count and largest sequence number. Our proposed algorithm has the field in addition to the fields of MAODV and is represented as follows.

Table 1. Trusted knowledge table

frd_msg	rev_msg	T_ip_addr	M_ip_addr

3.2 Phase 2: Calculate Effective Trust Value

The idea of "Trust" initially gets from sociologies and is characterized as the level of subjective conviction about the practices of a specific entity[18]. So in order to have better communication between mobile node and a fixed node, we are finding the trusted nodes so that the data can be protected from malicious nodes.

In this phase, the effective trust is calculated for the trusted nodes using hybrid method which is obtained by direct observation and recommendation based methods.

The direct trust value $[(DT]_{x,y})$ of node x on y is obtained by

$$DT_{x,y} = W(R_p) * R_p + W(R_q) * R_q + W(R_e) * R_e \quad (1)$$

Where W( ) is an assigned weight to event, R_p, R_q, R_e R_p, R_q, R_e are optimized route reply misbehavior factor, route request misbehavior factor, route error misbehavior factor respectively. The values of R_p, R_q, R_e can be determined as

$$R_p = \frac{R_{ps} - R_{pf}}{R_{ps} + R_{pf}};\ R_q = \frac{R_{qs} - R_{qf}}{R_{qs} + R_{qf}};\ R_e = \frac{R_{es} - R_{ef}}{R_{es} + R_{ef}} \quad (2)$$

Where R_{ps}, R_{qs}, R_{es} are the successful route reply acknowledgement packets, successful route request acknowledgement packets and successful route error acknowledgement packets respectively. Similarly R_{pf}, R_{qf}, R_{ef} are the numbers of failed packets.

The recommended trust value $[(RT]_{x,y})$ of node x on y is obtained by the recommendation of third node z as shown in figure 3.

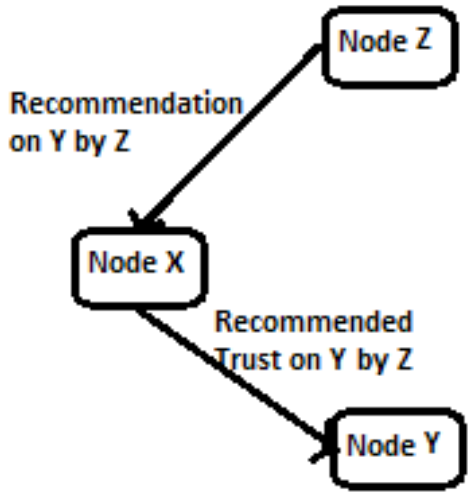

Figure 3. Recommendation based indirect trust establishment.

Now the effective trust value (ET_{xy}) is evaluated through hybrid method as

$$ET_{x,y} = \left(\alpha DT_{x,y} + \beta RT_{x,y}\right)/2 \quad (3)$$

where α and β are constants such that α + β = 1.

Effective Trusted Knowledge Algorithm

1. Initialize the mobile nodes (m_1 to m_n) and fixed nodes (f_1 to f_n).
2. Initialize (frd_msg=0, rev_msg=0, trusted_nodes=0, mal_nodes=0)
3. **if(** frd_msg ≠ rev_msg && threshold_value =max)
4. then M_ip_addr=ip_addr;
5. **else** T_ip_addr=ip_addr;
6. broadcast(M_ip_addr) ∀ (m_1 to m_n)
7. $R_p = \frac{R_{ps} - R_{pf}}{R_{ps} + R_{pf}};\ R_q = \frac{R_{qs} - R_{qf}}{R_{qs} + R_{qf}};\ R_e = \frac{R_{es} - R_{ef}}{R_{es} + R_{ef}}$
8. $DT_{x,y} = W(R_p) * R_p + W(R_q) * R_q + W(R_e) * R_e$
   read $[(RT]_{x,y})$
9. return $ET_{x,y} = \left(\alpha DT_{x,y} + \beta RT_{x,y}\right)/2$

4. Simulation Results

The result of proposed work is carried out using the NS2 with the necessary extension and evaluated the PDR, delay with respect to number of nodes

Table 2. Simulation parameters used

Total Number of Nodes	100
Network Size	650 * 650
MAC	802.11e
communication range	250 mtrs
Simulation Time	60 sec.
Source of Traffic	CBR
Size of Packet	512 Bytes
Mobility Model	Random Way Point mobility
Nodes Speed	2,4,6 and 12 m/sec.

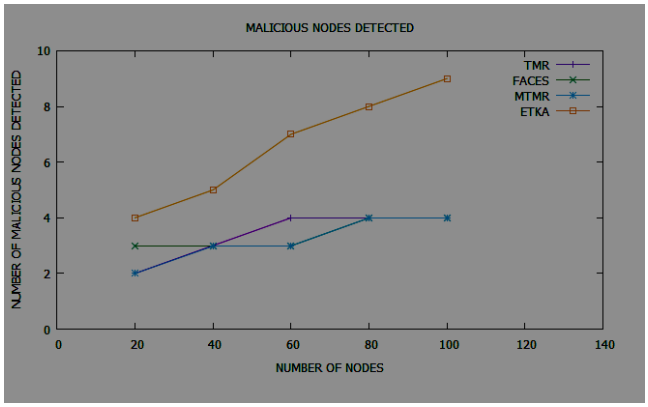

Figure 4. Malicious nodes detection with respect to number of nodes.

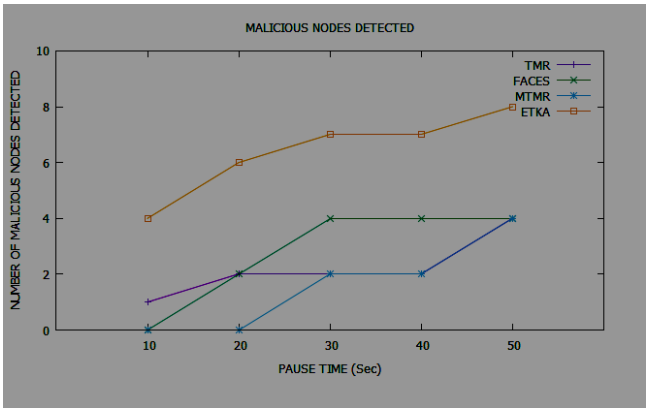

Figure 5. Malicious nodes detection with respect to mobility.

The quantity of vindictive nodes recognized in the system depicts the quality of the trusted routing method. In the Figure 4 and Figure 5, it is observed that ETKA finds large number of malicious nodes as it uses node observation followed by effective trust calculation with

hybrid method. If a node drops packets and the values in its trusted table does not matches with its neighbor nodes, it is declared malicious and then effective trust is calculated for the trusted nodes only. But other protocols Trust based Multipath Routing for Ad hoc Networks[20] (TMR), Message Trust based Multipath Routing for Ad hoc Networks[21] (MTMR) rely on the trust of a node and uses challenging the node for detecting malicious nodes. They set aside opportunity to arrive at a determination that a specific node is noxious. As we increment the quantity of network, more noxious nodes are distinguished by ETKA.

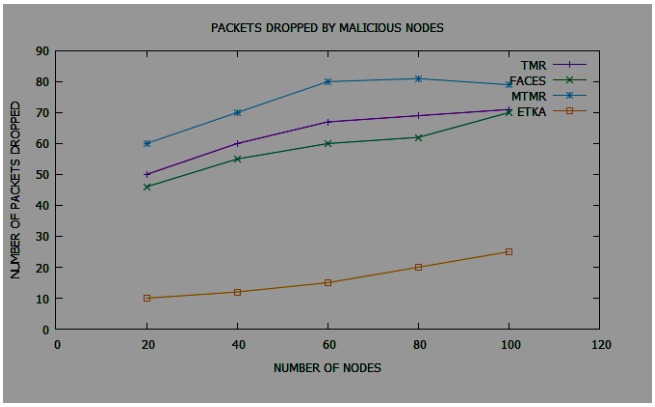

Figure 6. Packet drop evaluation by malicious nodes with respect to number of nodes.

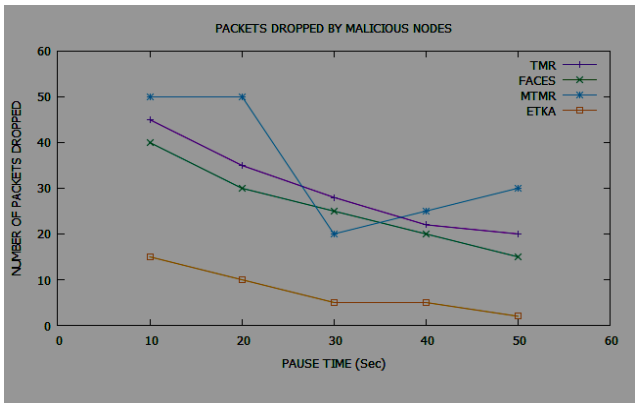

Figure 7. Packet drop evaluation by malicious nodes with respect to mobility.

In the Figure 6 and Figure 7, we can see that the packet drop is minimal in ETKA, as it productively removes the paths having untrusted nodes. Another multipath routing protocol discards a bigger quantity of packets as they go through a more noteworthy quantity of nodes and in this way expanding the odds of routing information through untrusted nodes. The increment in quantity of nodes or even the mobility is directly proportional to quantity of packets drop. As friends records are hard to keep up in a profoundly portable environment and observance presents a keen increment in the packet drop of FACES, whereas effectiveness is maintained in ETKA that provides better security in IIM compared to other three protocols.

5. Conclusion

This work proposed ETKA that enhances the security of integration of internet-MANET. Using node monitoring in promiscuous mode and we assess the trust estimations of trusted nodes in mobile ad hoc network. Mischievous activities, for example, dropping or changing packets can be recognized in our method by direct learning. Nodes having minimum trust qualities will be rejected using routing mechanism. Hence, a trusted route could be built up in mischievous situations. The aftereffects of IIM routing situation decidedly help the viability & execution of proposed method, that enhances throughput & Packet Delivery Ratio extensively, with marginally expanded normal overhead of messages and end-to-end delay. In future, the work can be extended by implementing using the concept of secret keys for encrypting the data to improve the security of communication in IIM.

6. References

1. Kumar R, Misra M, Sarje AK. An efficient gateway discovery in ad hoc network for internet connectivity. In the International Conference on Computational Intelligence and Multimedia Application, Institute of Electrical and Electronics Engineers (IEEE). 2007 Dec 13; 4:275–82.
2. Jisha G, Samuel P, Paul V. Role of gateway in MANET integration scenario. Indian Journal of Science and Technology. 2016 Jan; 9(3):1–19.
3. Global connectivity for IPv6 Mobile Ad Hoc Network [Internet]. 2001 [cited 2001 Nov 14]. Available from: http://www.cs.ucsb.edu/~ebelding/txt/globalv6.txt.
4. Manoharan R, Mohanalakshmie S. A trust based gateway selection scheme for integration of MANETs with internet. In Recent Trends in Information Technology (ICRTIT), International Conference on Institute of Electrical and Electronics Engineers (IEEE); 2011 Jun 3. p. 543–8.

5. Boukerch A, Xu L, El-Khatib K. Trust-based security for wireless ad hoc and sensor network. Computer Communication. 2007 Sep 10; 30(11):2413–27.
6. Kagal L, Finin T, Joshi A. Trust-based security in pervasive computing environment. Computer. 2001 Dec; 34(12): 154–7.
7. Sarvanko H, Höyhtyä M, Katz M, Fitzek F. Distributed resource in wireless network: discovery and cooperative uses. In Fourth European Research Consortium for Informatics and Mathematics (ERCIM) Workshop on E mobility; 2010 May. p. 51.
8. Ayachi MA, Bidan C, Abbes T, Bouhoula A. Misbehavior detection using implicit trust relation in the AODV routing protocol. In Computational Science and Engineering (CSE). International Conference on Institute of Electrical and Electronics Engineers (IEEE). 2009 Aug 29; 2:802–8.
9. Hamidian A, Körner U, Nilsson A. Performance of internet access solution in mobile ad hoc network. In International Workshop of the Euro NGI Network of Excellence. Springer Berlin Heidelberg; 2004 Jun 7. p. 189–201.
10. Dhurandher SK, Obaidat MS, Verma K, Gupta P, Dhurandher P. FACES: friend-based ad hoc routing using challenge to establish securities in MANETs system. Institute of Electrical and Electronics Engineers (IEEE) Systems Journal. 2011 Jun; 5(2):176–88.
11. Siddiqua A, Sridevi K, Mohammed AA. Preventing black hole attack in MANETs using secure knowledge algorithm. In Signal Processing And Communication Engineering Systems (SPACES), International Conference on Institute of Electrical and Electronics Engineers (IEEE); 2015 Jan 2. p. 421–5.
12. Amit Kumar Gupta ,Naveen Kumar Gupta, Rakesh Kumar. An efficient secure gateway selections and authentication scheme in MANET. International Journal of Advanced Research in Computer Science and Software Engineering. 2014 February; 4(2):11–18.
13. Shabut AM, Dahal KP, Bista SK, Awan IU. Recommendation based trust model with an effective defense scheme for MANETs. Institute of Electrical and Electronics Engineers (IEEE) Transactions on Mobile Computing. 2015 Oct 1; 14(10):2101–15.
14. Xi CH, Liang S, JianFeng MA, Zhuo MA. A trust management scheme based on behavior feedback for opportunistic network. China Communications. 2015 Apr; 12(4):117–29.
15. Zhang Y, Wang L, Sun W. Trust system design optimization in smart grid networks infrastructures. Institute of Electrical and Electronics Engineers (IEEE) Transactions on Smart Grid. 2013 Mar; 4(1):184–95.
16. Zhang Y, Wang L, Sun W, Green II RC, Alam M. Distributed intrusion detection system in a multi-layer networks architecture of smart grid. Institute of Electrical and Electronics Engineers (IEEE) Transactions on Smart Grid. 2011 Dec; 2(4):796–808.
17. Wang B, Soltani S, SHAPIRO J, Tan PN. Local detection of selfish routing behavior in ad hoc network. Journal of Interconnection Network. 2006 Mar; 7(01):133–45.
18. Cook KS. Russell sage foundation series on trust New York. Trust in Society. 2003 Feb; 2.
19. Hamidian A, Körner U, Nilsson A. Performance of internet access solutions in mobile ad hoc network. In International Workshop of the Euro NGI Network of Excellence Springer Berlin Heidelberg; 2004 Jun 7. p. 189–201.
20. Narula P, Dhurandher SK, Misra S, Woungng I. Security in mobile ad-hoc network using soft encryption and trust-based multi-path routing. Computer Communication. 2008 Mar 5; 31(4):760–9.
21. Dhurandher SK, Mehra V. Multi-path and message trust-based secure routing in ad hoc network. In Advance in Computing, Control and Telecommunication Technology. ACT'09. International Conference on Institute of Electrical and Electronics Engineers (IEEE); 2009 Dec 28. p. 189–94.