Josh Kumar *et al. EURASIP Journal on Wireless Communications and Networking* (2015) 2015:143
DOI 10.1186/s13638-015-0370-x

EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT

Jebakumar Mohan Singh Pappaji Josh Kumar[1,2], Ayyaswamy Kathirvel[3*], Namaskaram Kirubakaran[5], Perumal Sivaraman[6] and Muthusamy Subramaniam[4]

Abstract

Recent years have witnessed the increasing efforts toward making architecture standardization for the secured wireless mobile ad hoc networks. In this scenario when a node actively utilizes the other node resources for communicating and refuses to help other nodes in their transmission or reception of data, it is called a selfish node. As the entire mobile ad hoc network (MANETs) depends on cooperation from neighboring nodes, it is very important to detect and eliminate selfish nodes from being part of the network. In this paper, token-based umpiring technique (TBUT) is proposed, where every node needs a token to participate in the network and the neighboring nodes act as umpire. This proposed TBUT is found to be very efficient with a reduced detection time and less overhead. The security analysis and experimental results have shown that TBUT is feasible for enhancing the security and network performance of real applications.

Keywords: MANET; Selfish node; Performance and token-based umpiring technique (TBUT)

1 Introduction

Recent years have witnessed the increasing efforts toward making architecture standardization for the secured wireless mobile ad hoc networks. Actually, the framework of secured mobile ad hoc networks (MANETs) is an important part of the next-generation network design [1-4]. Such an improved security network brings a bright foreground for large data communications, i.e., the demand for the large data applications like IPTV, VoIP, and video conference has grown tremendously [5-8]. Meanwhile, research topic on secured communications has also received much attention in the past decade, and many works have been proposed to design robust and efficient schemes for delivering secured content delivery over error-prone networks [1,5,6,9-13].

This paper is based on the foundations of two systems proposed by Kathirvel and Srinivasan, namely self-umpiring system (SUS) [5,14] and enhanced triple umpiring system (ETUS) [1,5]. In the self-umpiring system, each node is issued with a token at the inception. The token consists of two fields: NodeID and status [5]. NodeID is assumed to be unique and deemed to be beyond manipulation and status is a single-bit flag. Initially, the status bit is preset to zero, indicating a green flag. The token with a green flag is a permit issued to each node, which confers it the freedom to participate in all network activities. Each node in order to participate in any network activity, say, Route Request (RREQ), has to announce its token. If its status bit is "1" indicating a "red flag," the protocol does not allow the node to participate in any network activity. The working of the self-umpiring system is explained with reference to Figure 1.

In the self-umpiring system, all the nodes have dual roles - packet forwarding and umpiring. In the forward path during data forwarding, each node monitors the performance of its immediate next node. That way, mobile node A can tell correctly whether mobile node B is forwarding the packet sent by it, by promiscuously hearing mobile node B's transmissions. Similarly during reply process RREP, mobile node C can verify whether mobile node B is unicasting the Route Reply (RREP) and whether the hop count given by mobile node B is correct. Thus, during forward path, mobile node A is the umpire for mobile node B and mobile node C is the umpire for mobile node B during reverse path operations. When a node is found to be misbehaving, say dropping data packets, the corresponding umpire immediately changes the status bit of guilty node to "1" indicating a red flag.

* Correspondence: ayyakathir@gmail.com
[3]Department of Information Technology, Anand Institute of Higher Technology, Chennai 603103, India
Full list of author information is available at the end of the article

Springer © 2015 Josh Kumar et al.

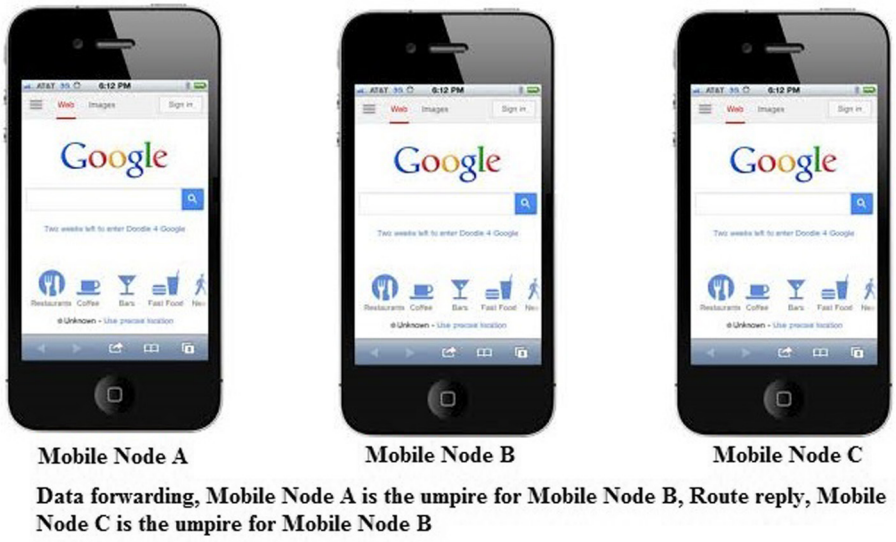

Figure 1 Self-umpiring system model.

The ETUS model [1,5] is presented in Figure 2. The active path is specified by node source, node 1, . . node N_{i-1}, node N_i . . node N_m, and the destination node. Thus, there are N_{m+2} nodes in the active path U_1, U_2 . . U_i , U_{i+1} . . U_m and U_{m+1} are umpiring nodes. Umpire U_i is situated in the communication zones of nodes N_i, N_{i-1}, U_{i-1}, and U_{i+1}. For node N_i, the two umpires will be U_i and U_{i+1}. The third umpire will be N_{i-1} in the forward path and N_{i+1} in their reverse path. Thus, when N_i is found to be misbehaving, say dropping packets or changing Hop count or sequence number, umpire nodes U_i, U_{i+1}, and N_{i-1} in the forward path and N_{i+1} in the reverse path send a M-ERROR message to the source and set the status bit of guilty node N_i to "1" indicating a red flag by M-Flag message. In these above two papers, we do not concentrate on selfish node. In this paper, token-based umpiring technique (TBUT) is proposed to detect and eliminate the selfish nodes efficiently in MANET. The main reason for using tokens in this analysis is to accelerate the detection and elimination of misbehaving selfish nodes. In MANET, nodes need to help other nodes to forward the data packets, but selfish nodes failed to do it. Because of selfishness of some nodes, the network performance may be reduced drastically.

A selfish node is a node that utilizes its limited resources, such as battery power, CPU time, and memory space purely for its own purpose. Because of its energy

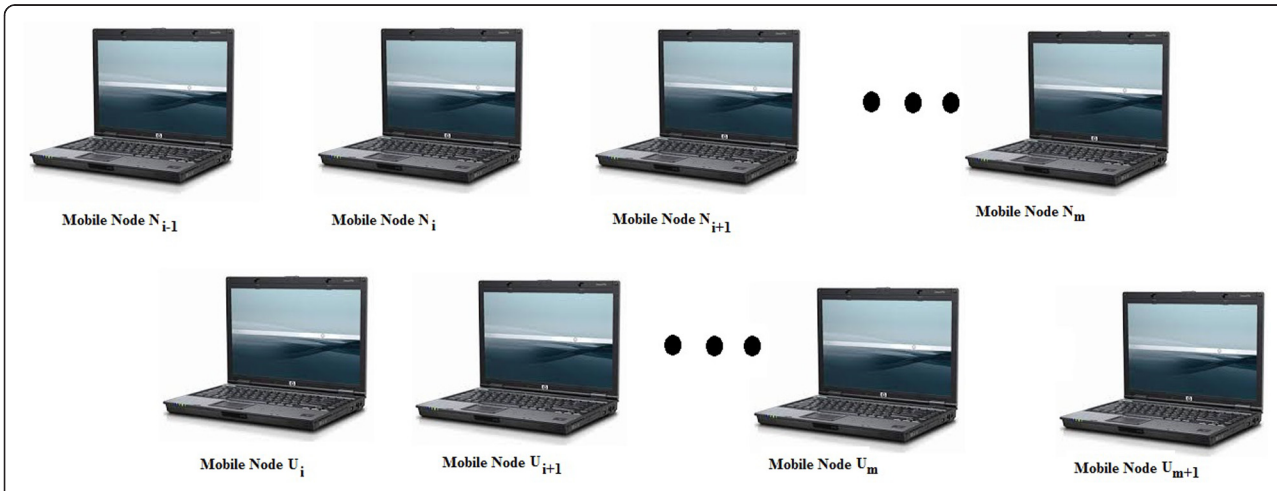

Figure 2 Enhanced triple umpiring system model.

and storage constraints, all incoming data forwarding and route discovery packets are intensely not accepted by it, thereby it tries to save its own resources. The features of the selfish nodes are not forwarding the routing packets, not replying to the hello messages, postponing the route discovery packets, and not forwarding the data packets. The main objective of the proposed work is too detected and eliminates the selfish node in MANET using TBUT. The proposed method consists of a packet dropping detection mechanism and a selfish node quarantining mechanism. In packet dropping detection mechanism, the selfish node is traced and identified. A selfish node quarantine mechanism envisages marking the offending nodes so that they do not participate any further in the network activities. In this paper, we will explain our proposed TBUT. The rest of the paper is organized as follows: Section 2 provides models and assumptions, Section 3 gives an overview of the proposed model, Section 4 gives simulations and experimental results, in Section 5 we explore the related work, and Section 6 draws up conclusions.

2 Models and assumptions

In this section, we formulate the MANET network and security model and also describe the selfish attacks.

2.1 Network model

We consider a MANET consisting of an unhindered number of wireless mobile nodes. For differentiation between nodes, we require each node to have a unique non zero identification (ID) number. Assumptions made in the design of the TBUT are as follows:

1. A MANET where nodes are free to move about or remain stand still at their will is assumed.
2. Each node may join or leave the network at any time.
3. Nodes may fail at any time.
4. The source and the destination node are not selfish nodes.
5. Every node in the network have neighbor list.
6. There exists a bi-directional communication link between any pair of nodes, which is a requirement for most wireless MAC layer protocols including IEEE 802.11 for reliable transmission.
7. Wireless interfaces support promiscuous mode of operation. Most of the existing IEEE 802.11-based wireless cards support such promiscuous mode of operations, to improve routing protocol performance.

The promiscuous mode, operation may incur additional communication overhead and energy utilization in order to process the transit packets. We do not address the energy efficiency in this work.

2.2 Security model

MANETs are vulnerable to security attacks due to their features of shared radio channel, insecure open medium, dynamic changing topology, lack of cooperative algorithms and centralized monitoring, limited resource availability, and physical vulnerability. Attacks on MANET can be classified into two categories, namely active attacks and passive attacks. An active attack attempts to destroy or alter the data packets and routing messages being exchanged in the network and it is very harmful to the network security. Passive attack does not disrupt the operation of the network. Our work focuses on passive attack, but we do not address nodes that eavesdrop and record other node transmissions, and we address only the selfish nodes that refuse to fully participate in the network routing operations. Our security model is implemented on top of the popular ad hoc on-demand distance vector (AODV) routing protocol.

3 Token-based umpiring technique

In the TBUT, each node is issued with a token at its inception. The token consists of three fields: NodeID, status, and reputation. NodeID is assumed to be unique and deemed to be beyond manipulation; status is a single-bit flag. Initially, the status bit is preset to zero indicating a green flag. Initially, reputation value is zero, i.e., positive. The token with a green flag and positive reputation is a permit issued to each node, which confers it the freedom to participate in all network activities. Each node in order to participate in any network activity, say Route Request RREQ, has to announce its token status bit and reputation value. If token status bit is "1" indicating a "red flag," protocol does not allow the node to participate in any network activity. Similarly, if reputation value is "−1" indicating a "negative reputation," the protocol does not allow the node to participate in any network activity. Our study does not depend on the exact mobile node structure of the networks. For the sake of the result explanation, it will be assumed that the network consists of approximately 100 mobile nodes span in the flat space (i.e., its span size is roughly 1 km^2) and that there are roughly 20 mobile nodes per service area region [7].

In the TBUT, all the nodes have dual roles - packet forwarding and umpire quarantining. In the forward path during data forwarding, each node monitors the performance of its immediate next node. That way, node A can tell correctly whether B is forwarding the packet sent by it, by promiscuously hearing B's transmissions. Similarly during the reply process RREP, C can verify whether B is unicasting the route reply RREP and whether the hop count given by B is correct [14]. Thus, during forward path, A is the umpire for B and C is the umpire for B during reverse path operations. When a node is found to be selfishly misbehaving, say dropping

packets, the corresponding umpire immediately sends a M-ERROR message to the source and the status bit of guilty node is set to "1" - red flag using M-Flag message and reputation value is set to −1. In order to correctly correlate the overheard messages, an additional field next_hop has been introduced in all routing messages as done in ETUS [5]. Though there are several kinds of misbehaviors that could be captured by promiscuous hearing, we are focusing only on selfish actions - dropping packets and not transmitting packets.

Our aim in designing the security system is to limit the overhead to as minimum as possible while getting a good improvement in throughput. The active path is specified by node source, node 1, . . node N_{i-1}, node N_i . . node N_m, and the destination node. Thus, there are N_{m+2} nodes in the active path U_1, U_2 . . U_{i-1}, U_{i+1}, . . U_m and U_{m+1} are umpiring nodes. Umpire U_i is situated in the communication zones of nodes N_i, N_{i-1}, U_{i-1}, and U_{i+1}. For node N_i, the two umpires will be U_i and U_{i+1}. The third umpire will be N_{i-1} in the forward path and N_{i+1} in their reverse path. Thus, when N_i is found to be misbehaving, say dropping packets or not forwarding control packets, umpire nodes U_i, U_{i+1}, and N_{i-1} in the forward path and N_{i+1} in the reverse path sends a M-ERROR message to the source then sets the status bit of guilty node N_i to "1" indicating red flag by M-Flag message and reputation value is set to −1. There are some other connected issues, which are being discussed in later sections.

3.1 Implementation of TBUT

We implement generic selfish attacks in TBUT on top of traditional AODV protocol, but its principal is applicable to other routing protocols as well. We modify the famous AODV routing protocol and add a new field, next_hop, in the routing messages, so that a node can correlate the overheard packets correctly. It is based on two algorithms. Algorithm 1 describes route discovery procedure and algorithm 2 describes selfish node quarantine procedure. Each node in order to participate in any network activity, says RREQ, RREP, and data forwarding, has to announce its token status and reputation value. If the node status bit is "1" indicating a red flag and negative reputation value, the protocol does not allow the node to participate in any network activity.

3.1.1 Route discovery

Routing algorithms are important for the functionality of a network because they provide paths on which the packets are sent over the network [15]. Route discovery allows any node in a MANET to dynamically discover a new route to any other node in MANET. The initial step of route discovery is to find the number of mobile nodes with the indicated token status position required to form the route to the destination. A node initiating a route discovery broadcasts a RREQ packet, which may be received by those nodes within wireless a transmission range, and the RREQ packet will be further forwarded till it reaches the destination. Once the destination is found, the initiating node receives a RREP packet listing a sequence of wireless network hops as shown in the Figure 3. Thus, a route is discovered between the source node and the destination node.

In the umpiring routine, a set of "*k*" umpiring nodes is used to convict the selfish node in packet forwarding operation. The steps of operation that should be taking place at umpiring routines are

- Destination node D should appoint first umpire node. The destination node D forwards its list of neighbors to the previous node;

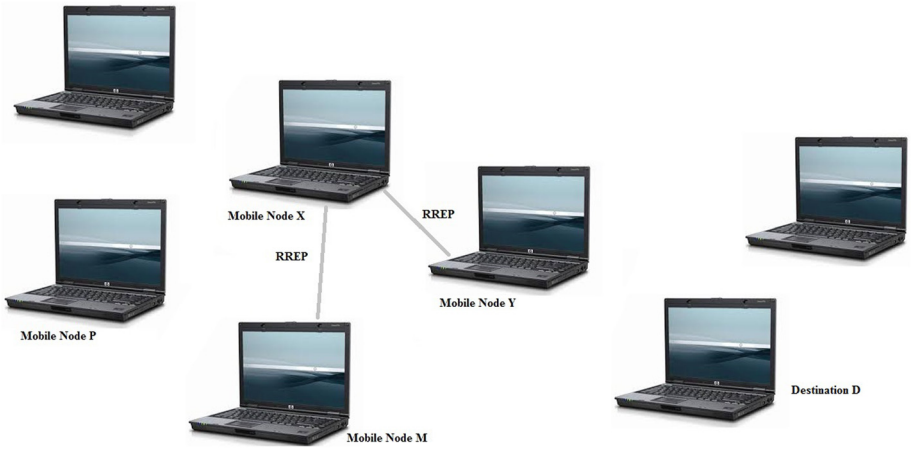

Figure 3 Each node can umpire the network activities of its neighbors by reputation of the overheard routing updates.

- The previous node has its own list of neighbors. Now, a previous node finds intersection of destination node and its own list of neighbors.
- From among the intersection nodes, it appoints one node as umpire;
- The umpire so appointed sends its neighbor list to the previous node and its adjacent umpire node;
- We find the intersection of neighbor list from the previous node and umpire node. The new intersection list of neighbors is sent to the next previous node;
- This operation is continued till the intersection list of neighbors reaches the source.

3.1.2 Selfish quarantine

The selfish quarantine mechanism in TBUT, the routing, and packet forwarding operations of each wireless node is done in a fully decentralized and localized manner. Each node overhears the channel in the promiscuous listening mode. Moreover, neighboring nodes and umpiring nodes cooperate with each other to improve the monitoring accuracy. During route discovery mobile, node X announces a new routing table update toward destination D with hop count as 1, claiming that its next hop is mobile node Y. Mobile node M can readily detect this routing misbehavior, because based on the route announced by mobile node Y, it can predict the correct distance from mobile node X to D via mobile node Y to be 3. The same idea can be applied to examine other fields in the routing updates as well.

Similarly during packet forwarding, when it overhears one packet sent to its neighbor wireless node, say mobile node P, it checks the buffer of the route entries announced by mobile node P and determines the next hop node to which mobile node P should forward the packet. If it has not overheard the packet being forwarded by mobile node P to the correct next hop node after a certain time, it considers this packet as being dropped. If the number of packets dropped by mobile node P exceeds a threshold value, mobile node M considers this as a selfish node and sets the status flag to "1" then turns the reputation value as negative and quarantines the particular node.

4 Simulations and results

We investigate the management of trust records by simulation that reveals an important insight into the effects of several attack methods presented earlier in the paper [5]. The simulation is set up as follows [16]. We use a simulation model based on QualNet 5.0 [17,18] in our evaluation. Our performance evaluations are based on the simulations of 100 wireless mobile nodes that form a wireless ad hoc network over a rectangular (1000 × 1000 m) flat space. The MAC layer protocol used in the simulations is the distributed coordination function (DCF) of IEEE 802.11 [18]. The performance setting parameters are given in Table 1.

Before the simulation, we randomly selected 30% of the network population as selfish behavior nodes. Each flow did not change its source and destination for the lifetime of a simulation run. We have kept the simulation time as 1000s, so as to enable us to compare our results with that of ETUS.

4.1 Packet delivery ratio

In the world of MANET, packet delivery ratio has been accepted as a standard measure of throughput. Packet delivery ratio is nothing but a ratio between the numbers of packets received by the destinations to the number of packets sent by the sources. We present in Figure 4 the packet delivery ratios for the scenario of 30% selfish node with node mobility varying between 0 and 20 m/s (Figure 5). Packet delivery ratio versus number of node in presence of 30% selfish node.

4.2 Failure to detect (false negative) probability

Failure to detect probability (false negative) is an important issue for supporting dependability in distributed network systems to guarantee continuous, safe, secure, and dependable operation [4]. Figure 6 presents failure to detect probability as a function of mobility and percentage of selfish nodes of TBUT and ETUS, respectively. A false-negative probability, which is the chance that umpires fail to convict and isolate a selfish node, can be defined as the ration of the number of selfish nodes left undetected to the total number of selfish nodes. We have calculated the failure to detect probability by taking into consideration only those nodes that took part in the network activity. Other researchers have also adopted the same approach. From Figure 6, we can see that the false negative probability has decreased in TBUT compared to ETUS.

Table 1 Parameter setting

Simulation parameters	Values
Simulation time	1000 s
Transmission range	250 m
Bandwidth	2 Mbps
Movement model	Random way point
Propagation model	Two-ray ground reflection
Maximum speed	0–20 m/s
Pause time	0 s
Traffic type	CBR
Payload size	512 bytes

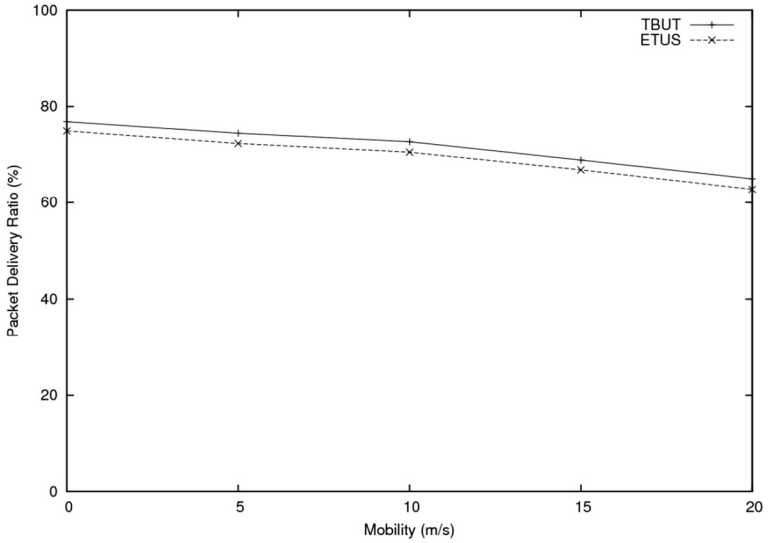

Figure 4 Packet delivery ratios, for 30% selfish node with node mobility varying between 0 and 20 m/s.

4.3 False accusation (false positive) probability

False accusation probability is the chance that umpires incorrectly convict and isolate a legitimate node. In other words, this is the probability of wrongly booking innocent nodes. Figure 7 presents false accusation probability as a function of mobility and percentage of selfish nodes for TBUT and ETUS, respectively. We find a similar decrease in false accusation probability at all other combinations of selfish node percentages and mobility values with ETUS. We find that false-positive probability increases with increasing percentage of selfish nodes and increased mobility. We present a comparison of false-positive probability values between TBUT and ETUS of 30% selfish nodes in Figure 7. It is seen that with ETUS, false-positive probabilities decrease slightly.

4.4 Communication overhead

Communication overhead (Figure 8) can be evaluated based on the number of transmissions of control messages like RREQ, RREP, and RERR in the case of plain AODV and in addition M_ERROR, M-Flag, umpire, and neighbor list messages in the TUS and ETUS (refer to Table 2).

4.5 Analysis of results

We find that TBUT yields a much higher packet delivery ratio compared to Self_USS, ETUS, and plain AODV in

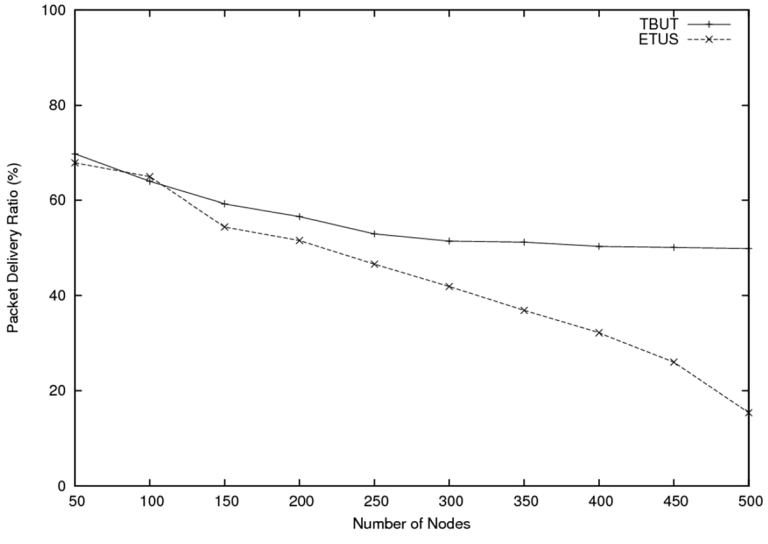

Figure 5 Packet delivery ratios versus number of node in the presence of 30% selfish node.

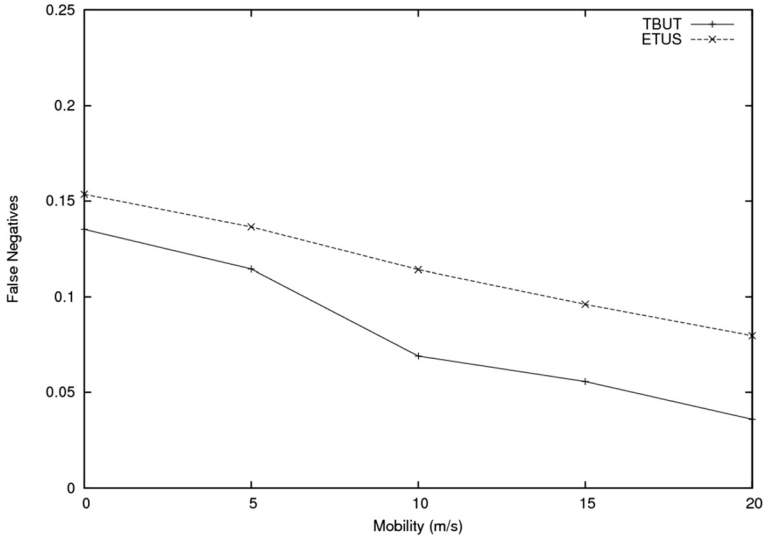

Figure 6 False negative, for 30% selfish node with node mobility varying between 0 and 20 m/s.

the presence of 30% selfish nodes in Table 3. It is found that with TBUT, there is a higher packet delivery ratio ranging from 3% (ETUS 20 m/s mobility) to 6% (Self_USS, 0 m/s mobility).

We present a comparison of communication overhead for Self_USS, ETUS, TBUT, and plain AODV in the presence of 30% selfish nodes in Table 2. It is found that with TBUT, there is a decrease in the communication overhead ranging from 26.05% (Self_USS, 0 m/s mobility) to 15.60% (Self_USS, 20 m/s mobility). However, TBUT communication overhead is much higher compared to Self_USS. For example, with a mobility of 20 m/s, ETUS communication overhead is 17.21% as compared to Self_USS. As compared with ETUS and TBUT, our proposed TBUTs have less communication overhead. We find that our proposed TBUTs yield a much higher output as compared to all other system.

5 Related works

The key distribution center (KDC) architecture is the main stream in wired network because KDC has so many merits: efficient key management, including key generation, storage, and distribution and updating. The lack of a trusted third party (TTP) key management scheme is a big problem in ad hoc network [1,5]. Different types of attacks on MANET were discussed by Abhay Kumar Rai et al. [19]; they have designed a security mechanism by which they can minimize or completely remove many of

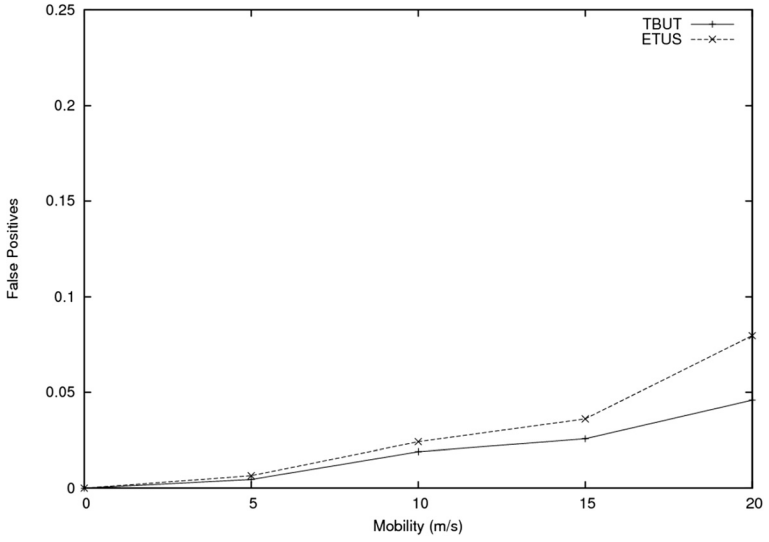

Figure 7 False positive, for 30% selfish node with node mobility varying between 0 and 20 m/s.

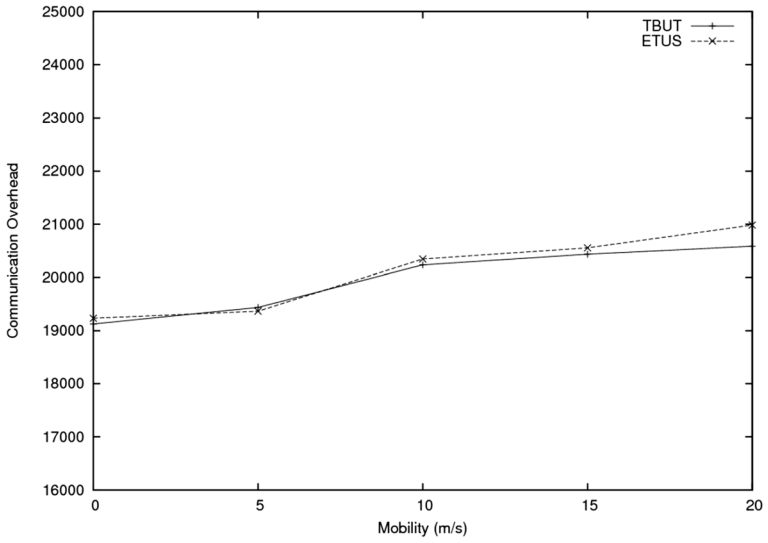

Figure 8 Communication overhead, for 30% selfish node with node mobility varying between 0 and 20 m/s.

those attacks. Sudha Rani et al. [20] proposed a detection and prevention of wormhole attack in stateless multicasting. Their scheme has no central administrator. They have shown that their schemes can handle wormhole attacks.

Leonidas Georgiadia et al. [21] made a survey of threats and possible solutions for resource allocation and cross-layer control in wireless networks. Raj et al. [22] proposed a solution for black hole attacks. It was implemented in prominent AODV protocol-based MANET. Tsou [23] developed a novel scheme BDSR to avoid black hole attack based on proactive and reactive architecture. Yu et al. [2] proposed a solution of a distributed and cooperative black hole node detection and elimination mechanism. Solda et al. [24] gave a solution for blacklisting attacks; in these papers, they studied the problem of forecasting attack sources based on past attack logs from several contributors. They formulated this problem as an implicit recommendation system [25,26].

Hernandez et al. [27] introduced a fast model to evaluate the selfish node detection in MANET using a watchdog approach. They estimated the time of detection and the overhead of collaborative watchdog approach for detecting one selfish node. Singh et al. [28] implemented a security-based algorithmic approach in MANETs. In this analysis, an empirical and effective approach was proposed to optimize the packet loss frequency. Jyoshna et al. [29] proposed a solution for byzantine attacks in ad hoc networks using SMT protocol that provides a way to secure message transmission by dispersing the message among several paths with minimal redundancy. Megha Arya and Yogendra Kumar Jain [30] gave a solution for gray hole attack. They use an intrusion detection system (IDS) to monitor the network or system, for selfish activities or policy violation, and produce reports to a management station. It takes over the sending of packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighbor nodes that try to send packets over attacking nodes lose the connection to destination, then they may want to discover a route again by broadcasting RREQ messages [31-34].

B.B. Jayasingh and B. Swathi [35] proposed a mechanism that detects the jellyfish attacks at a single node and that can be effectively deployed at all other nodes in the ad hoc network. They gave a solution that detects the jellyfish reorder attack based on the reorder density which is a basis for developing a metric.

Table 2 Communication overhead for Self_USS, plain AODV, ETUS, and TBUT

Mobility (m/s)	Communication overhead for selfish node = 30%			
	Self_USS	Plain AODV	ETUS	TBUT
0	14142	13136	19234	19125
5	15010	13603	19366	19436
10	15813	14082	20345	20234
15	16639	14580	20553	20433
20	17372	15082	20984	20584

Table 3 Throughput for Self_USS, plain AODV, ETUS, and TBUT

Mobility (m/s)	Throughput for selfish node = 30%			
	Self_USS	Plain AODV	ETUS	TBUT
0	72.22	50.44	74.92	76.83
5	70.04	42.18	72.32	74.45
10	68.25	30.89	70.52	72.69
15	64.58	28.55	66.85	68.88
20	60.46	26.07	62.78	64.98

Timothy et al.'s [36] paper focuses on jamming at the transport/network layer. Jamming at this layer exploits AODV and TCP protocols and is shown to be very effective in simulated and real networks when it can sense victim packet types, but the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing, and sequence is available to the attacker for sensing [19].

Kurkure and Chaudhari [37] illustrated a comparative analysis of the selfish node detection methods based on detection time and message overhead. In this paper, a collaborative watchdog method was used to identify the selfish nodes and diminish the detection time and message overhead. Sahu and Sinha [38] suggested a cooperative approach for understanding the behavior of IDS in MANETs. In this paper, they described about various attacks and techniques used for intrusion detection which were proposed to provide high performance. Patel et al. [39] used an AODV protocol for trust-based routing in ad hoc networks. Ad hoc networks have limited physical security, less infrastructure, restricted power supply, mobility network, and changing network topology [40-44]. Jawhar et al. suggested a reliable routing protocol for enhanced reliability and security of communication in the MANET and sensor networks [45].

Various P2P media streaming systems have been deployed successfully, and corresponding theoretical investigations have been performed on such systems [46]. In this paper, [47] thoroughly investigates the evolutionary dynamics of soft security mechanism, namely reciprocity-based incentive mechanism, in P2P systems based on evolutionary game theory (EGT). By soft security mechanism, it means social control mechanisms to overcome peers' selfish (rational) behaviors and encourage cooperation in P2P systems.

Trust management plays an important role in IoT [48-54] for reliable data fusion and mining, qualified services with context awareness, and enhanced user privacy and information security [9]. It helps people overcome perceptions of uncertainty and risk and engages in user acceptance and consumption on IoT services and applications [9,55,56]. However, current literature still lacks a comprehensive study on trust management in IoT [9]. Authenticated key agreement protocol is a useful cryptographic primitive, which can be used to protect the confidentiality, integrity, and authenticity for transmitted data over insecure networks [6].

Built upon opportunistic routing and random linear network coding, CodePipe not only simplifies transmission coordination between nodes but also improves the multicast throughput significantly by exploiting both intra-batch and inter-batch coding opportunities [10]. In particular, four key techniques, namely LP-based opportunistic routing structure, opportunistic feeding, fast batch moving, and inter-batch coding, are proposed to offer substantial improvement in throughput, energy efficiency, and fairness [10].

In the paper, [11] proposes a multi-constrained QoS multicast routing [12] method using the genetic algorithm. The proposal will be flooding limited [13] using the available resources and minimum computation time in a dynamic environment. By selecting the appropriate values for parameters such as crossover, mutation, and population size, the genetic algorithm improves and tries to optimize the routes.

For the author of this paper [57], they consider the assignment strategy with topology preservation by organizing the mesh nodes with available channels and aim at minimizing the co-channel interference in the network. The channel assignment with the topology preservation is proved to be NP-hard and to find the optimized solution in polynomial time is impossible. They have formulated a channel assignment algorithm named as DPSO-CA which is based on the discrete particle swarm optimization and can be used to find the approximate optimized solution [57,58].

All the above schemes only try to protect the system from the attacker, but not bother about quarantining attackers [3,16,59]. The TBUT systems not only detect the mischievous nodes but also prevent their further participation in the network.

6 Conclusions

The security considerations in a TBUT setting are still in their infancy phase and require a more thorough analysis by the research community. The misbehavior of selfish nodes is a major problem in wireless MANET. The selfish nodes do not participate in the routing and data transmission process, which intentionally drop the packets. These misbehaviors of the selfish nodes will impact availability, efficiency, reliability, and fairness. The selfish node utilizes the resources for its own purpose, and it neglects to share the resources to other nodes. So, it is important to detect the selfish nodes in MANET. We have conducted simulation studies to evaluate the performance of TBUT in the presence of 30% selfish nodes and have compared it with ETUS routing protocols. The results show that TBUT significantly improves the performance of ETUS in all metrics, packet delivery ratio, and control overhead. The security analysis and experimental results have shown that TBUT is feasible for enhancing the security and network performance of real applications. In the following, a number of potential research directions are introduced.

6.1 A. Cross-layer security schemes

Different layers in the MANETs need the authentication for their different functionalities. It is then possible to integrate the authentication from higher layers into the

MAC-PHY layer. This approach will save the cost of communication and provide a unifying framework to address the authentication of sensing nodes as well as the sensing data, among other possibilities.

6.2 B. Reliable spectrum schemes

Perhaps, solutions to combat attacks against TBUT schemes have been studied more than any other security issues. Still a thorough analysis to compare and contrast existing techniques, such as trust weight fusion versus consensus-based algorithms, can provides further insights into the pros and cons of each scheme and might lead future researchers toward developing more robust solutions.

6.3 C. Incentive-based security schemes

We classified the agents posing security threats in a TBUT into three categories, namely adversaries, malicious nodes, and silent nodes. Each group will follow a different attack strategy. It is interesting to address the incentives for misbehaviors and attack against a TBUT so as to adopt incentive minimization schemes. As an example, a silent node is seeking to further enhance its own performance at the expense of other network nodes. Thus, fair resource allocation strategies will ensure that no single node can sustain superior performance in the network, which in turn eliminates the opportunity of misbehavior based on fraudulent reports. Our future work will focus on improving the TBUT performance, by minimizing the innocent node booking. Last but not least, several interesting open problems are pointed out with possible addressing ideas to trigger more research efforts in this emerging area.

Competing interests

The authors declare that they have no competing interests.

Author's information

1. Mr. J.P.Josh Kumar was born on 13th September 1982 at Palayamkottai, Tamilnadu, India. He received his B.E. degree from Raajas Engineering College, Manonmanium Sundaranar University, Tirunelveli, Tamilnadu, India in 2003 and M.Tech. Degree from Sathyabama Institute of Science and Technology, Sathyabama University, Chennai, India in 2005. He immediately joined as Assistant Professor at Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai and worked there for Six years. Then he joined as Assistant Professor at GKM College of Engineering and Technology, Chennai in 2011 and is currently working there.
He has guided more than 20 U.G and P.G Projects. He has presented 7 papers in various national and international conferences. He has also published a paper in a reputed journal. He got award for "Best Teaching Methodology" while teaching at Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai. He is currently pursuing PhD in the area of "Mobile Ad Hoc Networks" at Sathyabama University, Chennai since December 2012 under the able guidance of Dr. A. Kathirvel, Professor and Head of Information Technology, Anand Institute of Higher Technology, Chennai.
2. Dr. A. Kathirvel was born in Erode, Tamilnadu, India. He received his B.E. degree from V.M.K.V. Engineering College, University of Madras, Chennai, in 1998, M.E. degree from Crescent Engineering College, University of Madras, Chennai, in the year 2002 standing 7th rank in the university. He got University Medalist and Best Project Award in his PG Degree studies. He got a doctoral degree from Anna University, Chennai, in 2010. He has got teaching, research, and administrative experience for more than 17 years in various engineering colleges, autonomous institutions, and universities.
He is currently working as Professor and Head of Information Technology at Anand Institute of Higher Technology, Chennai. He has worked as lecturer, senior lecturer, assistant professor, professor, and professor and head in various institutions. He has published more than 90 papers in national and international conferences and in international journals. He is working as scientific and editorial board member of many journals. He has reviewed dozens of papers in many journals. He has authored three books. He has also published a research monograph from the LAP Lambert Academic Publishing GmbH & Co., Germany, Europe, based on his Ph.D thesis titled "Umpiring Security Model and Performance improvement on MANETS," costing 110.35 Euros. His other two books are Introduction to GloMoSim and Prevention of Attacks using Umpiring Security Model for MANETS, LAP Lambert Academic Publishing GmbH & Co., Germany, Europe.
He is a life member of the ISTE (India), Senior Member IACSIT (Singapore), Life Member IAENG (Hong Kong), Member ICST (Europe), IAES, Member IEEE, and ACM. He has given a number of guest lecturers/expert talks and seminars, workshops, and symposiums. He has visited Dubai, Abu Dhabi, and Oman for presentation of his research papers in various international conferences. His biography was published in the 29th edition of Marquis's Who's Who in the World in 2012 issue. He has also guided more than three dozens of projects (B.E/B.Tech/M.E/M.Tech/MCA) in various engineering colleges. He has given many keynote/invited talks/ plenary lecturers in various national and international conferences and chaired many sessions. His research interests are protocol development for wireless ad hoc networks, security in ad hoc network, data communication and networks, mobile computing, wireless networks, and delay tolerant networks.

Author details

[1]Sathyabama University, Chennai 600119, India. [2]Department of ECE, G K M College of Engineering and Technology, Chennai 600063, India. [3]Department of Information Technology, Anand Institute of Higher Technology, Chennai 603103, India. [4]Department of Information Technology, S.A. Engineering College, Chennai 600077, India. [5]St. Peters University, Chennai 600054, India. [6]VIT University, Vellore 632014, India.

Received: 29 January 2015 Accepted: 24 April 2015
Published online: 23 May 2015

References

1. A Kathirvel, R Srinivasan, ETUS: enhanced triple umpiring system for security and robustness of wireless mobile ad hoc networks. International Journal of Communication Networks and Distributed Systems **7**(1/2), 153–187 (2011)
2. Yu CW, Wu T-K, Cheng RH, Chang SC, "A distributed and cooperative black hole node detection and elimination mechanism for ad hoc network", PAKDD workshops, Nanjing, China, 22–25, May 2007.
3. N Kirubakaran, A Kathirvel, Performance improvement of security attacks in wireless mobile adhoc networks. Asian Journal of Information Technology **13**(2), 68–76 (2014)
4. X Naixue, AV Vasilakos, T Laurence, LS Yang, Y Pan, R Kannan, Y Li, Comparative analysis of quality of service and memory usage for adaptive failure detectors in healthcare systems. IEEE Journal on Selected Areas in Communications **27**(4), 495–509 (2009)
5. A Kathirvel, R Srinivasan, ETUS: an enhanced triple umpiring system for security and performance improvement of mobile ad hoc networks. International Journal of Network Management **21**(5), 341–359 (2011)
6. H Yang, Y Zhang, Y Zhou, F Xiaoming, H Liu, AV Vasilakos, Provably secure three-party authenticated key agreement protocol using smart cards. Computer Networks **58**, 29–38 (2014)
7. P Demestichas, VA Stavroulaki, L Magdalene, AV Vasilakos, M Theologou, Service configuration and traffic distribution in composite radio environments. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews **34**(1), 69–81 (2004)
8. L Zhou, H-C Chao, AV Vasilakos, Joint forensics-scheduling strategy for delay-sensitive multimedia applications over heterogeneous networks. IEEE Journal on Selected Areas in Communications **29**(7), 1358–1367 (2011)
9. Z Yan, P Zhang, AV Vasilakos, A survey on trust management for Internet of Things. Journal Network and Computer Applications **42**, 120–134 (2014)

10. Peng Li, Song Guo, Shui Yu and Vasilakos A.V, "CodePipe: an opportunistic feeding and routing protocol for reliable multicast with pipelined network coding", in the Proceedings IEEE INFOCOM, pp.100–108, 2012.
11. Y-S Yen, H-C Chao, R-S Chang, A Vasilakos, Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs. Mathematical and Computer Modelling **53**(11–12), 2238–2250 (2011)
12. Athanasios V. Vasilakos, Yan Zhang, Thrasyvoulos Spyropoulos, Delay tolerant networks: protocols and applications, CRC Press, 2011.
13. Wei Quan, Changqiao Xu, Vasilakos A.V, and Jianfeng Guan, "TB2F: Tree-bitmap and bloom-filter for a scalable and efficient name lookup in content-centric networking", IFIP Networking, pp.1–9, 2014.
14. A Kathirvel, R Srinivasan, Enhanced self umpiring system for security using salvaging route reply. International Journal of Computer Theory and Engineering **2**(1), 129–134 (2010)
15. C Busch, R Kannan, AV Vasilakos, Approximating congestion + dilation in networks via "quality of routing" games. IEEE Transactions on Computers **61**(9), 1270–1283 (2012)
16. D He, C Chen, S Chan, J Bu, AV Vasilakos, ReTrust: attack-resistant and lightweight trust management for medical sensor networks. IEEE Transactions on Information Technology in Biomedicine **16**(4), 623–632 (2012)
17. Network Simulator. Scalable networks technologies: QualNet simulator version 5.0.2. http://web.scalable-networks.com/
18. A Kathirvel, Introduction to GloMoSim (LAP Lambert Academic Publishing GmbH & Co. Germany, Europe, 2011)
19. KC Suresh, S Prakash, AE Priya, A Kathirvel, Primary path reservation using enhanced slot assignment in TDMA for session admission". The Scientific World Journal **2015**, 1–11 (2015)
20. L Sudha Rani, R Raja Sekhar, Detection and prevention of wormhole attack in stateless multicasting. International Journal of Scientific & Engineering Research **3**(3), 1–5 (2012)
21. L Georgiadia, MJ Neely, L Tassiulas, Resource allocation and cross-layer control in wireless networks. Foundations and Trends in Networking **1**(1), 1–444 (2006)
22. PN Raj, PB Swadas, DPRAODV: a dynamic learning system against blackhole attack in AODV based MANET". International Journal of Computer Science **2**, 54–59 (2009)
23. Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs" 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13–16, Feb. 2011.
24. AL Soldo, A Markopoulou, Blacklisting recommendation system: using spatio-temporal patterns to predict future attacks. IEEE Journals on Selected Areas in Communications **29**(7), 1423–1437 (2011)
25. A Kathirvel, R Srinivasan, Self umpiring system for security in wireless mobile ad-hoc network. Journal of Wireless Sensor Network **2**(3), 264–266 (2010)
26. A Kathirvel, R Srinivasan, A system of umpires for security of wireless mobile ad hoc network. International Arab Journal of e-Technology **1**(4), 129–134 (2010)
27. E Hernandez orallo, JC Cano, C Calafate, P Manzoni, A fast model for evaluating the detection of selfish nodes using a collaborative approach in MANETs. Wireless Personal Communication **74**(2/1), 1099–1116 (2014)
28. R Singh, P Singh, M Duhan, An effective implementation of security based algorithmic approach in mobile adhoc network. Human centric Computer Information Science **4**(6), 1–14 (2014)
29. G Jyoshna, K Yoga Prasad, Removal of byzantine attacks in ad hoc networks. International Journal of Advanced Research in Computer Engineering & Technology **1**(3), 272–276 (2012)
30. M Arya, YK Jain, Grayhole attack and prevention in mobile adhoc network. International Journal of Computer Applications **27**(10), 21–26 (2011)
31. A Kathirvel, R Srinivasan, Double umpiring system for security in mobile ad hoc networks. International Journal of Wireless Networks and Communications **2**(1 & 2), 67–78 (2010)
32. A Kathirvel, R Srinivasan, Enhanced triple umpiring system for security and performance improvement in wireless MANETS. International Journal of Communication Networks and Information Security **2**(2), 77–84 (2010)
33. A Kathirvel, R Srinivasan, Self_USS: a self umpiring system for security in mobile ad-hoc network. International Journal of Engineering and Technology **2**(2), 196–203 (2010)
34. A Kathirvel, R Srinivasan, A study on salvaging route reply for AODV protocol in the presence of malicious nodes. International Journal of Engineering and Technology **1**(2), 151–155 (2009)
35. BB Jayasingh, B Swathi, A novel metric for detection of jellyfish reorder attack on ad hoc network. BVICAM's International Journal of Information Technology **2**(1), 15–20 (2010)
36. Timothy X Brown, Jesse E. James and Amita Sethi, "Jamming and sensing of encrypted wireless ad hoc networks", University of Colorado at Boulder, Technical Report CU-CS-1005-06, pp. 1–13, 2010.
37. A Kurkure, B Chaudhari, Selfish node detection techniques in MANET: a review. International Journal of Comput Science and Management Research. **1**(1), 88–94 (2013)
38. L Sahu, C Sinha, A cooperative approach for understanding behavior of intrusion detection system in mobile ad hoc networks. International Journal of Comput Science **1**(1), 24–30 (2013)
39. DG Patel, PA Pandey, MC Patel, Trust based routing in ad-hoc networks. International Journal of Current Engineering Technology **4**(2), 860–863 (2014)
40. A Kathirvel, R Srinivasan, "Performance analysis of propagation model using wireless mobile ad hoc network routing protocols". International Journal of Wireless Communication **1**(1), 1–8 (2009)
41. A Kathirvel, R Srinivasan, "A system of umpires for security of MANET". International Journal of Networking and Communication Engineering **1**(1), 1–5 (2009)
42. A Kathirvel, R Srinivasan, Single umpiring system for security of mobile ad hoc networks. Journal of Advances in Wireless and Mobile Communications **2**(2), 141–152 (2009)
43. A Kathirvel, R Srinivasan, Triple umpiring system for security of mobile ad hoc networks. International Journal of Engineering and Information technology **1**(2), 95–100 (2009)
44. A Kathirvel, R Srinivasan, "Global mobile information system simulator in Fedora Linux". ACM Computer Communication Review **1**(1), 1–10 (2009)
45. I Jawhar, Z Trabelsi, J Al-Jaroodi, Towards more reliable and secure source routing in mobile ad hoc and sensor networks. Telecommunication System **55**, 81–91 (2014)
46. Z Shen, J Luo, R Zimmermann, AV Vasilakos, Peer-to-peer media streaming: insights and new developments. Proceedings of the IEEE **99**(12), 2089–2109 (2011)
47. Y Wang, A Nakaob, AV Vasilakosd, J Mae, P2P soft security: on evolutionary dynamics of P2P incentive mechanism. Computer Communications **34**(3), 241–249 (2011)
48. B Liu, J Bi, AV Vasilakos, Toward incentivizing anti-spoofing deployment. IEEE Transactions on Information Forensics and Security **9**(3), 436–450 (2014)
49. J Qi, AV Vasilakos, W Jiafu, L Jingwei, D Qiu, Security of the Internet of Things: perspectives and challenges. Wireless Networks **20**, 2481–2501 (2014)
50. M Kiranmayi, A Kathirvel, Underwater wireless sensor networks: applications, challenges and design issues of the network layer - a review". International Journal of Emerging Trends in Engineering Research **3**(1), 05–11 (2015)
51. D Mohanageetha, SK Muthusundar, M Subramaniam, A Kathirvel, Temporary redundant transmission mechanism for SCTP multihomed hosts. The Scientific World Journal **2015**, 11–21 (2015)
52. C Rajabhushanam, A Kathirvel, System of one to three umpire security system for wireless mobile ad hoc network. Journal of Computer Science **7**(12), 1854–1858 (2011)
53. A Kathirvel, M Subramaniam, C Rajabushanam, Burglar detecting system for wireless mobile ad hoc network. European Journal of Scientific Research **62**(1), 14–23 (2011)
54. A Kathirvel, R Srinivasan, Analysis of propagation model using mobile ad hoc network routing protocols. International Journal of Research and Reviews in Computer Science **1**(1), 7–14 (2010)
55. ZM Fadlullah, T Taleb, AV Vasilakos, M Guizani, N Kato, DTRAB: combating against attacks on encrypted protocols through traffic-feature analysis. IEEE/ACM Transactions on Networking **18**(4), 1237–1247 (2010)
56. Z Sheng, S Yang, Y Yu, AV Vasilakos, JA Mccann, KK Leung, A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities. IEEE Wireless Communications **20**(6), 91–98 (2013)
57. H Cheng, N Xiong, AV Vasilakos, LT Yang, G Chen, X Zhuang, Nodes organization for channel assignment with topology preservation in multi-radio wireless mesh networks. Ad Hoc Networks **10**(5), 760–773 (2012)
58. A Attar, H Tang, AV Vasilakos, Y Richard, A survey of security challenges in cognitive radio networks: solutions and future research directions. Proceedings of the IEEE **100**(12), 3172–3186 (2012)
59. Y Zeng, K Xiang, D Li, AV Vasilakos, Directional routing and scheduling for green vehicular delay tolerant networks. Wireless Networks **19**(2), 161–173 (2013)