Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 334-341, 2015
ISSN 1990-9233
© IDOSI Publications, 2015
DOI: 10.5829/idosi.mejsr.2015.23.ssps.201

A Novel Based Analysis of Baffled Traffic Patterns in MANETs

[1]P. Sathyaraj, [2]S. Rukmani Devi and [2]D. Kalpana

[1]RMK College of Engineering and Technology, India, [2]RMD Engineering College, India

Abstract: In this paper, we address the problem of providing STAR attack model. The Baffled traffic model is proposed to overcome the STARS attack. Control message is exchanged between each node in the region periodically. So the entry in the point to point matrix is 1 always. Simultaneously, the data is broadcasted to all the nodes in its region to confuse the traffic monitoring node.

Key words: Anonymous Communication • Mobile Ad Hoc Networks • Statistical Traffic Analysis

INTRODUCTION

Communication anonymity is a critical issue in MANETs, which generally consists of the following aspects: 1) Source/destination anonymity-it is difficult to identify the sources or the destinations of the network flows. 2) End-to-end relationship anonymity-it is difficult to identify the end to-end communication relations. To achieve anonymous MANET communications, many anonymous routing protocols such as ANODR, MASK and OLAR have been proposed. Though a variety of anonymity enhancing techniques like onion routing and mix-net are utilized, these protocols mostly rely on packet encryption to hide sensitive information (e.g., nodes' identities and routing information) from the adversaries.

However, passive signal detectors can still eavesdrop on the wireless channels, intercept the transmissions and then perform traffic analysis attacks. Over the past few decades, traffic analysis models have been widely investigated for static wired networks. For example, the simplest approach to track a message is to enumerate all possible links a message could traverse, namely, the brute force approach. Recently, statistical traffic analysis attacks have attracted broad interests due to their passive nature, *i.e.*, attackers only need to collect information and perform analysis quietly without changing the network behavior (such as injecting or modifying packets). The predecessor attacks and disclosure attacks are two representatives. However, all these previous approaches do not work well to analyze MANET traffic because of the following three natures of MANETs: 1) The broadcasting nature: In wired networks, a point-to-point message transmission usually has only one possible receiver. While in wireless networks, a message is broadcasted, this can have multiple possible receivers and so incurs additional uncertainty. 2) The ad hoc nature: MANETs lack network infrastructure and each mobile node can serve as both a host and a router. Thus, it is difficult to determine the role of a mobile node to be a source, a destination, or just a relay. 3) The mobile nature: Most of existing traffic analysis models does not take into consideration the mobility of communication peers, which make the communication relations among mobile nodes more complex.

In an evidence-based statistical traffic analysis model, every captured packet is treated as evidence supporting a point-to-point (one-hop) transmission between the sender and the receiver. A sequence of point-to-point traffic matrices is created and then they are used to derive end to-end (multihop) relations. This approach provides a practical attacking framework against MANETs but still leaves substantial information about the communication patterns undiscovered.

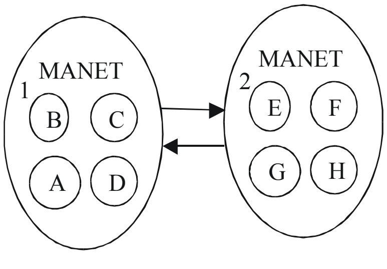

Fig. 1: Design of MANET Network

Corresponding Author: P. Sathyaraj, RMK College of Engineering and Technology, India.
E-mail: sathyarajece@rmkcet.ac.in - rdrukmani319@gmail.com - kalpana.cse@rmd.ac.in.

First, the scheme fails to address several important constrains (e.g., maximum hop-count of a packet) when deriving the end-to-end traffic from the one hop evidences. Second, it does not provide a method to identify the actual source and destination nodes (or to calculate the source/destination probability distribution). Moreover, it only uses a native accumulative traffic ratio to infer the end-to-end communication relations (e.g., the probability for node j to be the intended destination of node i is computed as the ratio of the traffic from i to j to all traffic coming out from node i) which incurs a lot of inaccuracy in the derived probability distributions.

Reusing the evidence-based model, a novel statistical traffic pattern discovery system (STARS) is enhanced. STARS aims to derive the source/destination probability distribution, *i.e.*, the probability for each node to be a message source/destination and the end to-end link probability distribution, *i.e.*, the probability for each pair of nodes to be an end-to-end communication pair. To achieve its goals, STARS includes two major steps: 1) Construct point-to-point traffic matrices using the time-slicing technique and then derive the end-to-end traffic matrix with a set of traffic filtering rules; and 2) Apply a heuristic approach to identify the actual source and destination nodes and then correlate the source nodes with their corresponding destinations.

Literature Review: Yang Qui [1] propose a novel STARS for MANETs. STARS are basically an attacking system, which only needs to capture the raw traffic from the PHY/MAC layer without looking into the contents of the intercepted packets. From the captured packets, STARS constructs a sequence of point-to-point traffic matrices to derive the end-to-end traffic matrix and then uses a heuristic data processing model to reveal the hidden traffic patterns from the end-to end matrix. Our empirical study demonstrates that the existing MANET systems can achieve very restricted communication anonymity under the attack of STARS.

Y-Zhang [6] proposed to enable both anonymous MAC layer and network-layer communications but focused only on the passive attack. A Boukerche [10] used a methodology of SDAR protocol for providing privacy and anonymity in ad hoc networks but it encrypted the routing packet header and abstaining from using unreliable intermediate nodes leads to routing.

Due to the nature of radio transmissions communications in wireless networks are easy to capture and analyze. Next to this, privacy enhancing techniques (PETs) proposed for wired networks such as the Internet often cannot be applied to mobile ad hoc networks (MANETs). In this paper [2] S.seys and B.preneel presented a novel anonymouson demandroutingscheme for MANETs. We identify a number of problems of previously proposed works and propose an efficient solution that provides anonymity in a stronger adversary model.

Anonymouscommunication methods, try to prevent traffic analysis attacks by hiding nodes' identities from outside observers. As a result, adversaries cannot find any correlation between observed traffic patterns and nodes' real information. In this paper, R. Shokri, M. yabandeh and N. Yazdani [3] have introduced Pseudo AODV protocol in which originidentifiersof nodes are replaced by randomly generated pseudonyms in ad hoc on demand distance vector (AODV) routing scheme. The main contribution of our protocol is improving AODV to provide sender/recipient and relationship anonymity with the least computational overhead. Simulation results shows the lower imposed overhead of our method in comparison with similar protocols.

M. Reed [5] describesanonymous connectionsand their implementation usingonionrouting. This paper also describes several application proxies for onion routing, as well as configurations of onion routing networks.

Onion routingis an infrastructure for private communication over a public network. It provides anonymous connections that are strongly resistant to both eaves dropping and traffic analysis. Onion routing 'sanonymous connections are bi-directional, near real-time and can be used anywhere a socket connectioncan be used. Any identifying information must be in the data stream carried over an anonymous connection. Anonionis a data structure that is treated as the destination address byonion routers; thus, it is used to establish an anonymous connection. Onions themselves appear different to eachonionrouter as well as to network observers. The same goes for data carried over the connectionsthey establish. Proxy-aware applications, such as Web browsers and e-mail clients, require no modification to useonionrouting and do so through a series of proxies. A prototypeonion routing network is running between our lab and other sites.

X.wang [12] investigated the fundamental limitations off low transformations in achieving anonymity and we show that flow transformations do not necessarily provide the level of anonymity people have expected or believed. By injecting unique watermark into the inter-packet timing domain of a packetflow, we are able to make any sufficiently longflowuniquely identifiable even if.

- It is disguised by substantial amount of cover traffic.
- It is mixed or merged with a number of otherflows.
- It is split into a number sub flows.
- There is a substantial portion of packets dropped.
- It is perturbed in timing due to either naturalnetworkdelay jitter or deliberate timing perturbation.

In addition to demonstrating the theoretical limitations of low-latency anonymous communications systems, he developed the first practical attackon the leading commerciallow-latency anonymous communication system. Our real-time experiments show that our flow water marking attackonly needs about 10 minutes active our analytical and empirical results demonstrate that achieving anonymity inlow-latency communication systems is much harder than we have realized and current flow transformation basedlow-latency anonymous communication systems need to be revisited.

Proposed System: To provide solution to the STARS attack model in MANET, We have proposed a new secure data transmission model named as Baffled Traffic model. This proposed model comprises the following modules

- Network Partition
- Detection of gateway node to reach the destination region
- Priority ordered control message exchange
- Broadcasting the data to the nodes in its region

Network Partition: Initially, the network region is partitioned into grid. In Figure 2, Let us say the horizontal width of the network area is x and the vertical height of the area is y. The identifier 'a' denotes each region's width and height. Then the Number of rows (NoR) in grid is given by;

$$NoR = \frac{x}{a}$$

Number of columns (NoC) is given by;

$$NoC = \frac{y}{a}$$

Number of grids (NoG) in a network region is given by;

$$NoG = NoR \times NoC$$

Detection of Gateway Node to Reach the Destination Region: Each and every node maintains its neighbor table along with its region number. The source node detects the route by using shortest path algorithm. Then extract the region number of the nodes in the route. For the next region to which the source node have to transmit the data, it will find the common node by analyzing the neighbor table. Then that gateway node detects the next gateway node dynamically. This process continues until reach the region of destination node.

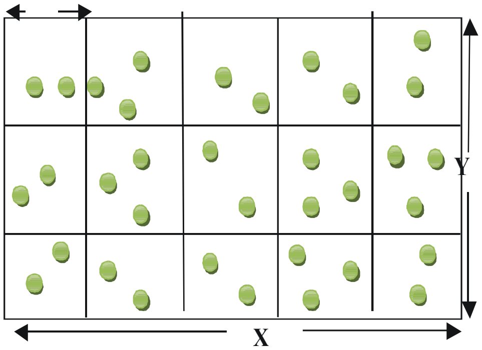

Fig. 2: Network Partitioning into Grids

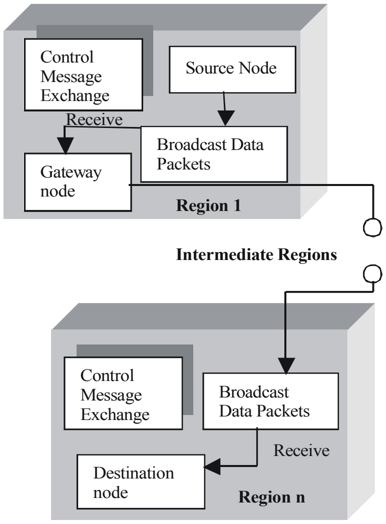

Fig. 3: Block diagram

Priority Ordered Control Message Exchange: In Figure 3, each and every node in our network region has to exchange the control information as flag value '1' or '0'. '1' indicates that node need to transmit data and '0' indicates that node is idle. After receiving flag message the Gate way node wait for data from that particular node which send the flag value 1. If the gateway node receives flag value 1 from more than one node in the sense, it will assign priority according to its urgency. It will broadcast the data to next region according to its priority. During the data transmission also the control message is exchanged between the nodes.

Broadcasting the Data to the Nodes in its Region: The source node broadcast the data in its region. The Gate way node broadcast the received data to the nodes in the next region to reach the destination. This process continues until reach the region of destination node. If the source and destination is in the same region means the source will send by broadcasting to its region.

Block Diagram of Baffled Traffic Model

System Design: We assume the anonymity enhancing techniques are used to protect the MANETs. However, these techniques are designed to different levels of anonymity. To focus on the statistical traffic analysis, we assume that a combination of these techniques is applied and the targeted MANET communication system is subject to the following model:

- The PHY/MAC layer is controlled by the commonly used 802.11(a/b/g) protocol. But all MAC frames (packets) are encrypted so that the adversaries cannot decrypt them to look into the contents.
- Padding is applied so that all MAC frames (packets) have the same size. Nobody can trace a packet according to its unique size.
- The "virtual carrier sensing" option is disabled. The source/destination addresses in MAC and IP headers are set to a broadcasting address (*i.e.*, all "1") or to use identifier changing techniques. In this case, adversaries are prevented from identifying point-to point communication relations.
- No information about the traffic patterns is disclosed from the routing layer and above.
- Dummy traffic and dummy delay are not used due to the highly restricted resources in MANETs.

Attack Model: The attackers' goal is to discover the traffic patterns among mobile nodes. Particularly, we have the following four assumptions for attackers:

- The adversaries are passive signal detectors, *i.e.*, they are not actively involved in the communications. They can monitor every single packet transmitted through the network.
- The adversary nodes are connected through an additional channel which is different from the one used by the target MANET. Therefore, the communication between adversaries will not influence the MANET communication.
- The adversaries can locate the signal source according to certain properties (e.g., transmission power and direction) of the detected signal, by using wireless location tracking techniques such as triangulation, nearest sensor, or RF fingerprinting. Note that none of these techniques can identify the source of a signal from several nodes very close to each other. Hence, this assumption actually indicates that the targeted networks are sparse in terms of the node density. In other words, any two nodes in such a network are distant from each other so that the location tracking techniques in use are able to uniquely identify the source of a wireless signal. In the following of this paper, unless specifically denoted as "signal source" or "source of signal," the word "source" indicates the source of a network flow.
- The adversaries can trace the movement of each mobile node, by using cameras or other types of sensors. In this case, the signals (packets) transmitted by a node can always be associated with it even when the node moves from one spot to another.

Simulation Tool

Network Simulator 2 (NS2): NS2 is one of the most popular open source network simulators. The original NS is a discrete event simulator targeted at networking research. In this section, we will give a brief introduction to the NS2 system. The simulation of STAR and protocol was done in NS-2.33, using the wireless extensions. This simulation environment offers high fidelity, as it includes full simulation of the IEEE 802.11 physical and MAC layers. The NS-2.33 wireless simulation model simulates nodes moving in an unobstructed plane. Motion follows the random waypoint model a node chooses a destination uniformly at random in the simulated region, chooses a velocity uniformly at random from a configurable range and then moves to that destination at the chosen velocity. Upon arriving at the chosen waypoint, the node pauses for a configurable period before repeating the same process. In this model, the pause time acts as a proxy for the degree of mobility in a simulation; longer pause time amounts to more nodes being stationary for more of the simulation.

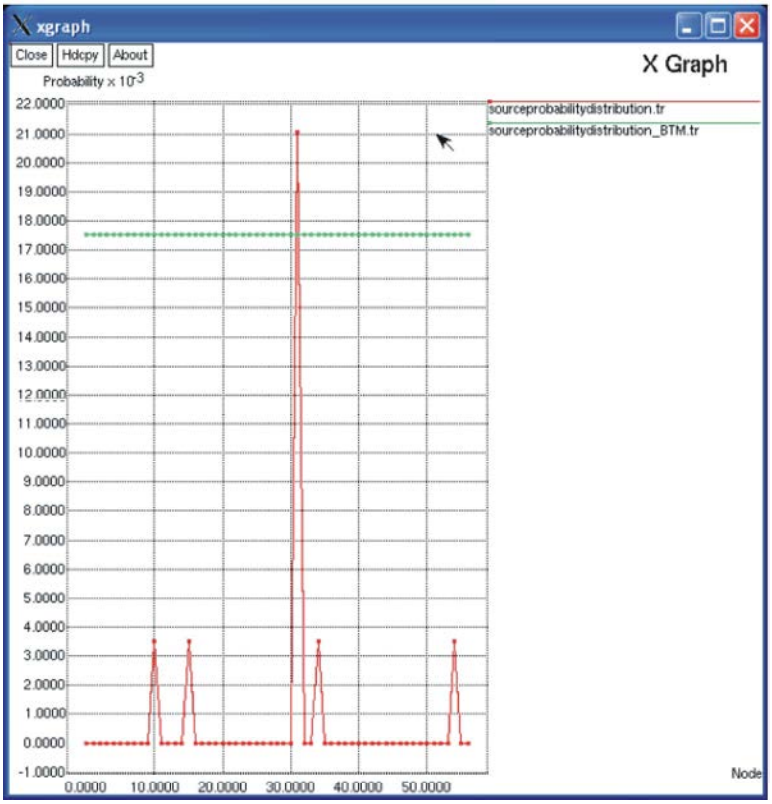

Fig. 4: Source Probability Distribution comparison of STAR and Baffled traffic analysis

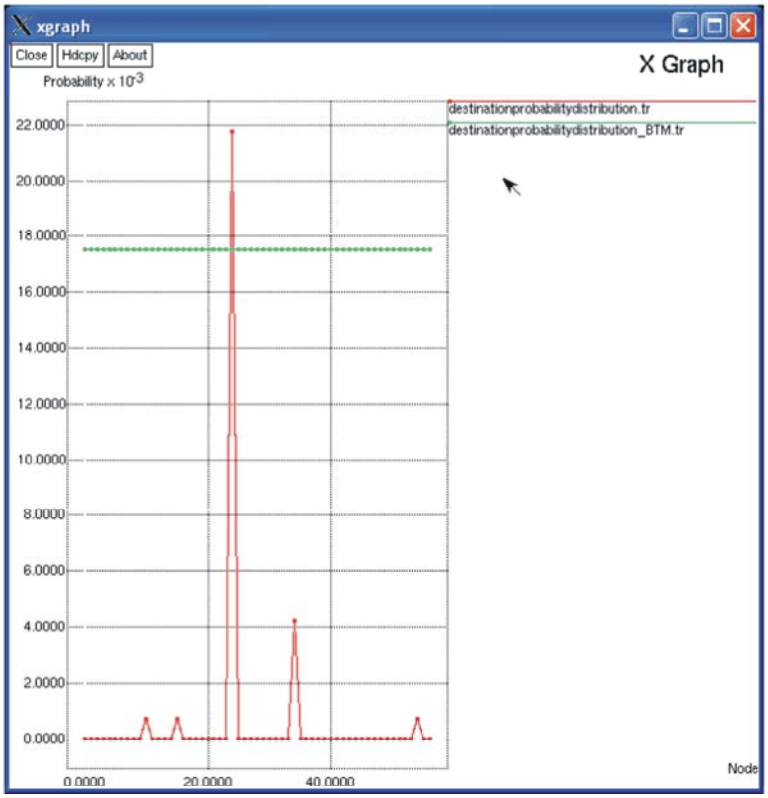

Fig. 5: Destination Probability Distribution comparison of STAR and Baffled traffic analysis

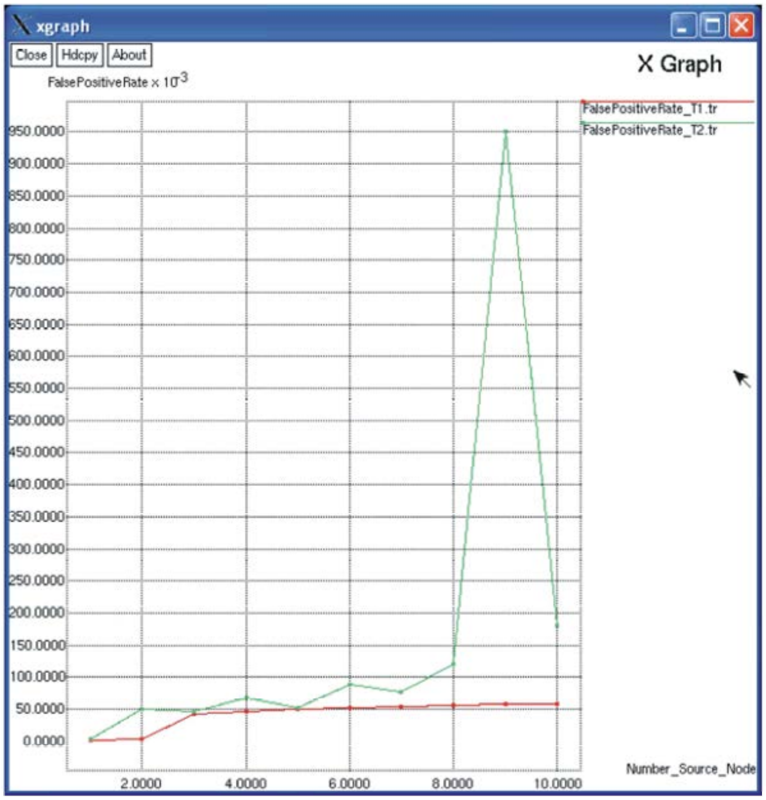

Fig. 6: False Positive Comparison of STAR and Baffled traffic analysis

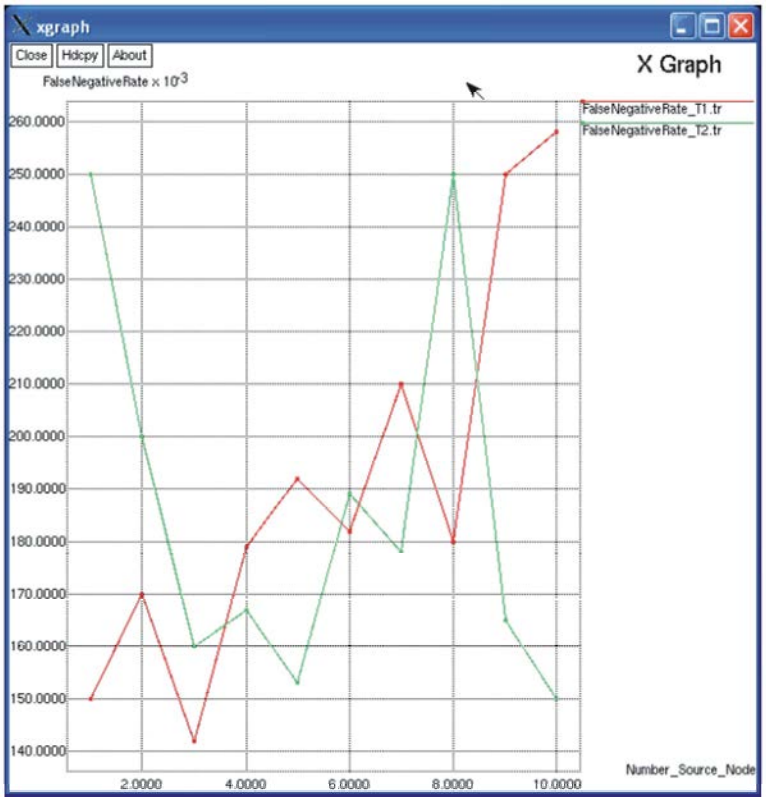

Fig. 7: False Negative Comparison of STAR and Baffled traffic analysis

CONCLUSION AND FUTURE ENHANCEMENT

In this work, we propose a new Baffled Traffic Model for MANETS. This proposed traffic model provides the solution against STARS attack model. The exchange of control message periodically, the Point to Point matrix result in the STARS attack model result that the probability value of each and every node will have same value. The data is also broadcasted to each and every node in its region. So, the attacker cannot predict the actual source and destination by using STARS attack model. The size of control message is one bit only, so it never leads to overhead among the nodes.

REFERENCES

1. Yang Qin, Dijiang Huang, Senior Member, IEEE and Bing Li, 2014. Student Member, IEEE STARS: A Statistical Traffic Pattern Discovery System for MANETs MARCH/APRIL.
2. Seys S. and B. Preneel, 2006. "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks," Proc. IEEE 20th Int'l Conf. Advanced Information Networking and Applications Workshops (AINA Workshops '06), pp: 133-137.
3. Shokri, R. M. Yabandeh and N. Yazdani, 2007. "Anonymous Routing in MANET Using Random Identifiers," Proc. Sixth Int'l Conf. Networking (ICN '07), pp: 2.
4. Song, R. L. Korba and G. Yee, 2005. "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks," Proc. Third ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '05), pp: 33-42.
5. Reed, M., P. Syverson and D. Goldschlag, 2002 "Anonymous Connections and Onion Routing," IEEE J. Selected Areas in Comm., 16(4): 482-494, May.
6. Kong, J., X. Hong and M. Gerla, 2007. "An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, 6(8): 888-902, Aug.
7. Zhang, Y., W. Liu, W. Lou and Y. Fang, 2006. "MASK: Anonymous On- Demand Routing in Mobile Ad Hoc Networks," IEEE Trans. Wireless Comm., 5(9): 2376-2385, Sep.
8. Qin Y. and D. Huang, 2008. "OLAR: On-Demand Lightweight Anonymous Routing in MANETs," Proc. Fourth Int'l Conf. Mobile Computing and Ubiquitous Networking (ICMU '08), pp: 72-79.
9. Blaze, M., J. Ioannidis, A. Keromytis, T. Malkin and A. Rubin, 2005. "WAR: Wireless Anonymous Routing," Proc. Int'l Conf. Security Protocols, pp: 218-232.
10. Boukerche K. El-Khatib, L. Xu and L. Korba, 2004. "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN '04), pp: 618-624.
11. Dai, W., 2007. "Two Attacks against a PipeNet-Like Protocol Once Used by the Freedom Service.
12. Wang, X., S. Chen and S. Jajodia, 2007. "Network F low Watermarking Attack on Low-Latency Anonymous Communication Systems," Proc. IEEE Symp. Security and Privacy, pp: 116-130.
13. Hanan Saleet, Rami Langar, Kshirasagar Naik, Raouf Boutaba, Amiya Nayak and Nishith Goel, 2001. 'Intersection-Based Geographical Routing Protocol for VANETs: A Proposal and Analysis', IEEE Transactions on Vehicular Technology, 60(9): 4560-4574.
14. Marcin Poturalski, Panos Papadimitratos and Jean-Pierre Hubaux, 2013. 'Formal Analysis of Secure Neighbor Discovery in Wireless Networks', IEEE Transactions on Dependable and Secure Computing, 10(6): 355-367.
15. Seon Yeong Han and Dongman Lee, 2013. 'An Adaptive Hello Messaging Scheme for Neighbor Discovery in On-Demand MANET Routing Protocols', 17(5): 1040-1043.
16. Adnan Abu-Mahfouz and Gerhard P. Hancke, 2013. 'Distance Bounding: A Practical Security Solution for Real-Time Location Systems', IEEE Transactions on Industrial Informatics, 9(1): 16-27.
17. Jie Yang, Yingying (Jennifer) Chen, Wade Trappe and Jerry Cheng, 2013. 'Detection and Localization of Multiple Spoofing Attackers in Wireless Networks', IEEE Transactions on Parallel and Distributed System, 24(1): 44-58.
18. Raquel Lacuesta, Jaime Lloret, Miguel Garcia and Lourdes Pen alver, 2013. 'A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation', IEEE Transactions on Parallel and Distributed Systems, 24(4): 629-641.
19. Mohammed Erritali, Oussam a Mohamed Reda and Bouabid El Ouahidi, 2012. 'IJARCSSE: UML Modelling of Geographic Routing Protocol 'GPSR' for its integration into the Java Network Simulator'.

20. Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu and Sy-Yen Kuo, 2013. 'Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks', IEEE Transactions on Information Forensics and Security, 8(5): 754-768.
21. Daojing He, Chun Chen, Sammy Chan, Jiajun Bu and Laurence T. Yang, 2013. 'Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks', IEEE Transaction on Industrial Electronics, 60(11): 5348-5354.
22. Shirina Samreen and G. Narasimha, 2012. 'An Efficient Approach for the Detection of Node Misbehaviour in a MANETs based on Link Misbehaviour', IEEE 3rd International Advanced Computing Conference, pp: 588-592.
23. Jiajia Liu, Xiaohong Jiang, Hiroki Nishiyama and Nei Kato, 2013. 'On the Delivery Probability of Two-Hop Relay MANETs with Erasure Coding', IEEE Transactionon Communications, 61(4): 1314-1326.
24. Kassem Fawaz and Hassan Artail, 2013. 'DCIM: Distributed Cache Invalidation Method for Maintaining Cache Consistency in Wireless Mobile Networks', IEEE Transaction on Mobile Computing, 12(4): 1314-1326.
25. Peng Zhao, Xinyu Yang, Wei Yu and Xinwen Fu, 2011. 'A Loose Virtual Clustering based Routing for Power Heterogeneous MANETs', IEEE Transaction on Vehicular Technology, 62(5): 2290-2302.
26. Kannan Govindan and Prasant Mohapatra, 2012. 'Trust Computations and Trust Dynamics in Mobile AdhocNetworks: A Survey', 14(2): 279-298.
27. Janusz Kusyk, Jianmin Zou, Stephen Gundry, Cem Safak Sahin and M. mit Uyar, 2012. 'Metrics for performance evaluation of self-positioning autonomous MANET nodes', IEEE Sarnoff Symposium, pp: 1-5.
28. Quansheng Guan, F. Richard Yu, Shengming Jiang and Victor C. M. Leung, 2012. 'Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks with Cooperative Communications', IEEE Transaction on Vehicular Technology, 61(6): 2674-2685.
29. Aldar C-F. Chan, 2012. 'Distributed Private Key Generation for Identity Based Cryptosystems in Ad Hoc Networks', IEEE Transactions on Wireless Communication, 1(1): 46-48.
30. Yingbin Liang, H. Vincent Poor and Lei Ying, 'Secrecy Throughput of MANETs Under.
31. Passive and Active Attacks' 2011. IEEE transactions on Information Theory, 57(10): 6692-6702.