International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 29797-29808

http://www.ripublication.com

# A Traffic Locality Oriented Second Route Discovery For Manets

**S. Vinoth, PG Scholar**
*Department of Electronics and Communication,*
*Velammal Institute of Technology,*
*Chennai, India, vinoth.bec@gmail.com*
**G. Shanmugaraj, Asst. Prof**
*Department of Electronics and Communication,*
*Velammal Institute of Technology,*
*Chennai, India, gsraj76@gmail.com*

## Abstract

Mobile ad hoc networks (MANETs) are collections of wireless mobile devices with restricted broadcast range and resources, and no fixed infrastructure. Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and from a security point of view. A novel route discovery algorithm called second route was also proposed, together with a claimed security proof within the same model. In this paper we show that the security proof for the route discovery algorithm second route is flawed, and that moreover this algorithm is vulnerable to a hidden STAR attack. We also analyze the security framework that was used for route discovery, and argue that compos ability is an essential feature for ubiquitous applications. We conclude by discussing some of the major security challenges for route discovery in MANETs. Recently, a security model tailored to the specific requirements of MANETs was on second route strategy.

**Index Terms:** Traffic matrix, Routing table, hidden traffic.

## Introduction

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as

applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering message must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing[4]. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network. An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. MANETs are self-organizing and self re-configuring multi hop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi hop forwarding[17]. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network.

In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes[7].

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to

become vulnerable to security breaches. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies.

Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network[11]. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources.

In ad hoc networks devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it.

There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing[14]. The second and more severe kind of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures.

The provision of systematic approaches to evaluate the impact of such threats on particular routing protocols remains an open challenge today. Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks[10]. The active attacks are further classified into internal attacks and external attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques. Internal attacks are from internal nodes which are actually authorized nodes and part of the network hence it is difficult to identify.

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links[19]. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks[1]. The design of network protocols for these networks is a

complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects[9]. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

## Proposed Scheme

In STAR system every captured packet is treated as an as an evidence supporting a point-to-point (one-hop) transmission between the sender and the receiver. Statistical traffic analysis intends to discover sensitive information from the statistical characteristics of the network traffic, for example, the traffic volume. The adversaries usually do not change the network behavior (such as injecting or modifying packets). The only thing they do is to quietly collect traffic information and perform statistical calculations[10]. Here an attacker finds himself to be on an anonymous path to the targeted destination, he increments the shared counter for its predecessor node in this path.

Number of techniques has been proposed based on packet encryption to protect the communication in MANETs, Still MANETs are vulnerable to certain statistical traffic analysis attacks. Thus present a Novel statistical traffic pattern discovery system (STARS). STARS functioning based on stastical characteristics of captured raw traffic. STARS discover the relationships of source to destination communication. Studies conclude STARS achieve good accuraccy in hidden traffic pattern

**Flow Diagram:**

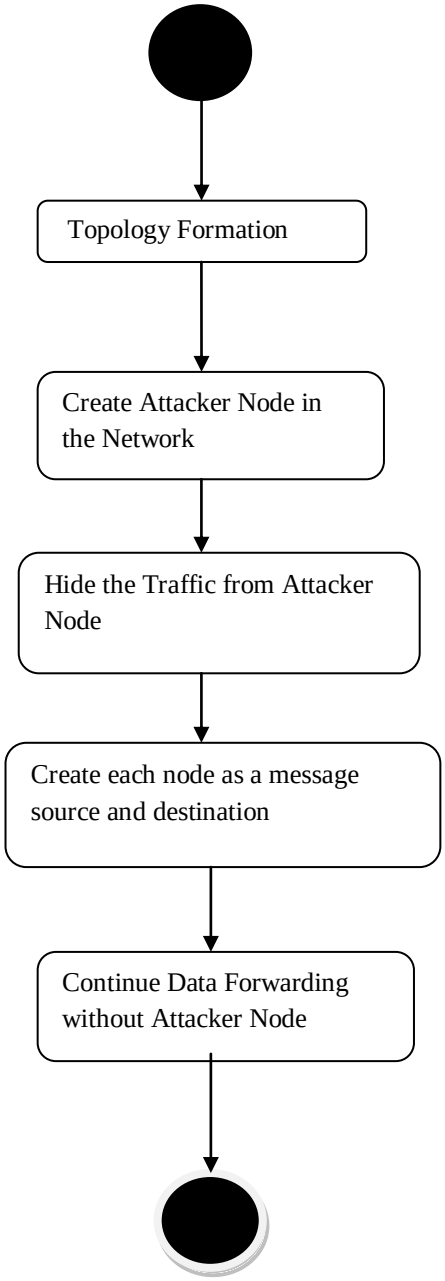



**Figure 1:** Flow diagram

STAR is a complete disclosure attack. It is apassive attack. It is hard to identify is the attack happen or not. STAR will completely monitor etair traffic and capture path of data flow.STAR is a complte target tracking mechanisam.It is a type of location disclosure attack.One way can say as external attack beacause it never effect any nodes.

*Modules*

1.Topology Formation
2.Attacker Model
3.STAR
4.Traffic Protector

*1.Topology Formation*

Initially we are placing nodes in the network and we choose a source and destination. If the source has no route to the destination, then source A initiates the route discovery in an on-demand fashion. After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination node[21]. If a closer neighbor node is available, the RREQ packet is forwarded to that node. If no closer neighbor node is the RREQ packet is flooded to all neighbor nodes.

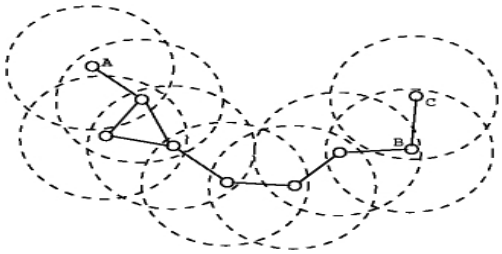



**Figure 2:** Topology Formation

When destinations receive the RREQ, it will generate RREP and it will send the same path. Finally we establish the route for data traffic.

*2. Attacker Model*

Here STARS including the attacker node which one monitors all the possible traffic patterns in the whole network. This attack is known as disclosure attack. Attackers only need to collect information and perform analysis quietly without changing the network behavior (such as injecting or modifying packets).

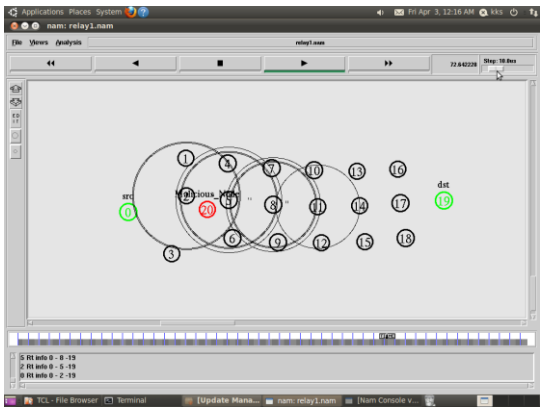


**Figure 3:** Attacker Model

*3. STAR*

STAR is the technique will create source/destination probability distribution for each and every node to be a message source and destination and the end-to-end link probability distribution(the probability for each node to be an end-to-end communication pair).

**Traffic Pattern Discovery Source/Destination Probability Distribution:**

The ability of STARS to identify the source and destination by calculating the source/destination probability distribution. The source probability distribution of (S1) and the destination probability distribution of (S2), are derived and the node with highest probability to be the destination, which match the simulation setup.

*4.Traffic Protector*

In this module, first it uses the captured traffic to construct a sequence of point-to-point traffic matrices and then derives the end-to-end traffic matrix. Second, further analyzing the end-to-end traffic matrix, it calculates the probability for each node to be a source/destination (the source/destination probability distribution) and that for each pair of node to be an end-to-end communication link (the end-to-end link probability distribution). Finally it will hide the traffic pattern between actual source and destination from disclosure nodes.

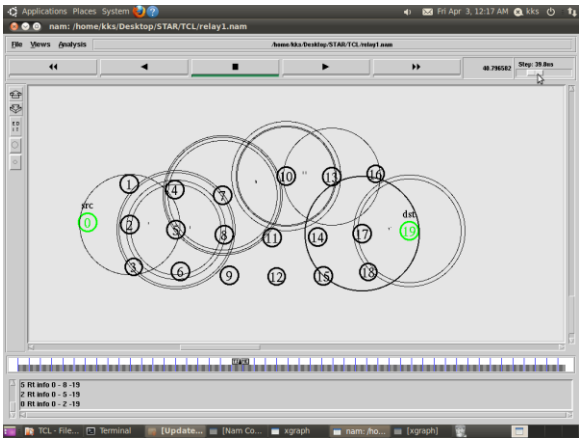


**Figure 4:** Traffic Matrices Construction

*Point-to-Point Traffic Matrix*

With the captured point-to-point (one-hop) traffic in a certain period T , we first need to build point-to-point traffic matrices such that each traffic matrix only contains independent packets. Thus packets captured at different time could be the same packet appearing at different locations, such as the two packets sent by node 1 and node 2 consecutively, so they are “dependent” on each other. To avoid a single point-to-point traffic matrix from containing two dependent packets, we apply a “time slicing” technique. Let the traffic matrix be $W_e$, which is an N _ N one-hop traffic relation matrix. The length of each time interval is determined by two criteria: 1) A node can

be either a sender or a receiver within this time interval. But it cannot be both. 2) Each traffic matrix must correctly represent the one-hop transmission during the corresponding time interval.

In this way, the construction of matrices Wj 1^1/4

ðW$_1$; W$_2$; . . . ; W$_K$ Þ will automatically involve mobility in the traffic matrices constructions.

That said, for the example given we could derive it as:

$$W = \begin{bmatrix} 2 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & & \\ 1 & ¼^4 & 0 & 0 & 0 & 5 \end{bmatrix}; \quad W0{:}5 = \begin{bmatrix} 2 & 0 & 0 & 0 & 3 \\ 0 & & 0 & 0{:}5 & : \\ 2 & ¼^4 & 0 & 0 & 0 & 5 \end{bmatrix}$$

*End-to-End Traffic Matrix*

Given a sequence of point-to-point traffic matrices our goal is to derive the end-to-end traffic matrix.

**Algorithm 1.**

1: R ¼ W$_1$
2: for e ¼ 1 to K _ 1 do
R ¼ gðR; W$_{eþ1}$Þ þ W$_{eþ1}$
3: end for
4: return R

In this algorithm, each update to R (line 3) includes the multi-hop traffic derivation function.

## Simulation Results

Simulating is a process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behavior of the system and/or evaluating various strategies for the operation of the system. Simulation is widely-used in system modeling for applications ranging from engineering research, business analysis, manufacturing planning, and biological science experimentation, just to name a few. Compared to analytical modeling, simulation usually requires less abstraction in the model (i.e., fewer simplifying assumptions) since almost every possible detail of the specifications of the system can be put into the simulation model to best describe the actual system. When the system is rather large and complex, a straightforward mathematical formulation may not be feasible. In this case, the simulation approach is usually preferred to the analytical approach.

In common with analytical modeling, simulation modeling may leave out some details, since too many details may result in an unmanageable simulation and substantial computation effort. It is important to carefully consider a measure under consideration and not to include irrelevant detail into the simulation.

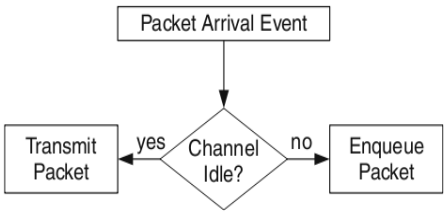



**Figure 5:** Packet Arrival Event

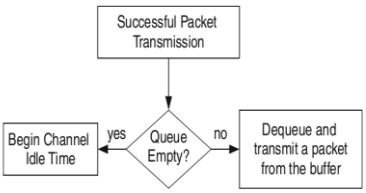
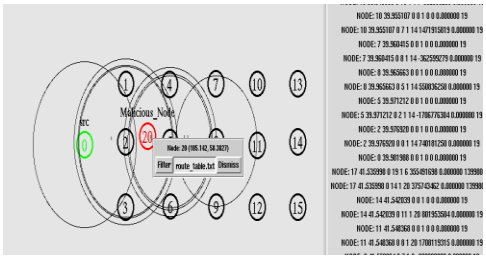
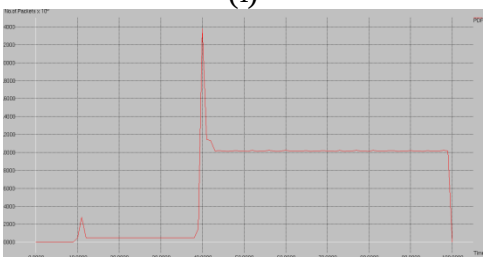



**Figure 6:** Successful Packet Transmission

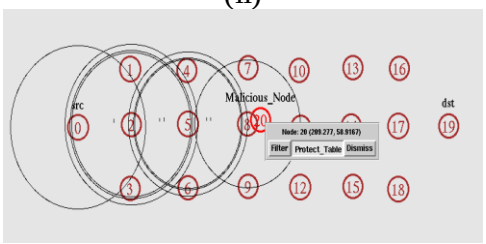
The following snap shots represent how nodes are created and data are transmitted with attacker node in (i) and(ii) and data transmission after the path is hidden in(iii) and (iv).



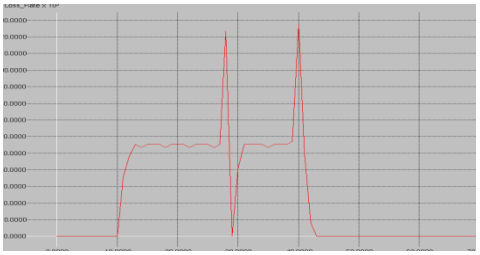
(i)



(ii)




(iii)



(iv)

## Conclusion

Source hiding technique was a type of traffic security method. In this system each point acts as source and destination. This was a form of originating point to point traffic. Thus a complete end to end anonymity will form. All this security is provided before the traffic will form. Thus prevention better than cure will come in practical. In STAR disclosure attack entire traffic path is captured. Source and destination have no idea about attack. This is a type of passive attack. Such a disclosure attack completely avoided through this source hiding security technique.

## References

[1]. J. Kong, X. Hong, and M. Gerla, "An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 6, no. 8, pp. 888-902, Aug. 2007.

[2]. Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.

[3]. Y. Qin and D. Huang, "OLAR: On-Demand Lightweight Anonymous Routing in MANETs," Proc. Fourth Int'l Conf. Mobile Computing and Ubiquitous Networking (ICMU '08), pp. 72-79, 2008.

[4]. M. Blaze, J. Ioannidis, A. Keromytis, T. Malkin, and A. Rubin, "WAR: Wireless Anonymous Routing," Proc. Int'l Conf. Security Protocols, pp. 218-232, 2005.

[5]. S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks," Proc. IEEE 20th Int'l Conf. Advanced Information Networking and Applications Workshops (AINA Work-shops '06), pp. 133-137, 2006.

[6]. R. Shokri, M. Yabandeh, and N. Yazdani, "Anonymous Routing in MANET Using Random Identifiers," Proc. Sixth Int'l Conf. Networking (ICN '07), p. 2, 2007.

[7]. R. Song, L. Korba, and G. Yee, "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, 2005.

[8]. M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing," IEEE J. Selected Areas in Comm., vol. 16, no. 4, pp. 482-494, May 2002.

[9]. D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, 1981.

[10]. J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability, pp. 10-29, 2001.

[11]. W. Dai, "Two Attacks against a Pipe Net-Like Protocol Once Used by the Freedom Service," http://weidai.com/freedom-attacks.txt, 2013.

[12]. X. Wang, S. Chen, and S. Jajodia, "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems," Proc. IEEE Symp. Security and Privacy, pp. 116-130, 2007.

[13]. M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transactions," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.

[14]. M. Wright, M. Adler, B. Levine, and C. Shields, "The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems," ACM Trans. Information and System Security, vol. 7, no. 4, pp. 489-522, 2004.

[15]. [15] A. Perrig, R. Canneti, D. Song, and J. D. Tygar, "The TESLA broadcast Authentication protocol," RSA Cryptobytes, vol. 5, no. 2, pp. 2-13, 2002.

[16]. [16] C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An efficient Identity based batch verification scheme for vehicular sensor networks," In Proc. of the 27th IEEE International Conference on Computer Communications (INFOCOM), pp. 24650, Phoenix, Arizona, USA, 2008.

[17]. [17] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An Efficient RSU aided Message Authentication Scheme in Vehicular Communication Networks," In Proc. of IEEE International Conference on Communications(ICC), Beijing, China, May 2008.

[18]. [18] C.P. Schnorr, "Efficient identification and signatures for smart cards," in Proc. of the 9th Annual International Cryptology Conference (Advances in Cryptology - CRYPTO), Santa Barbara, California , pp. 239–252, 1989.

[19]. [19] J. Freudiger, M. H. Manshaei, J.-P.Hubaux, and D. C. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in Proc.of ACM Conference on Computer and Communications Security, 2009, pp. 324–337.

[20]. [20]] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007.

[21]. [21] U.S. Department of Transportation, "National highway traffic safety administration," In Veh. Safety Commun.Project, Final Report. AppendixH: WAVE/DSRC Security, Apr. 2006.

[22]. [22] W. Susilo, F. Zhang, and Y. Mu, "Identity-based strong designated verifier signature schemes," in Proc. of the 9th Australasian Conference on Information Security and Privacy (ACISP), Sydney, Australia, pp.313–324, 2004.

[23]. [23] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," In Proc. of the 30th IEEE International Conference on Computer Communications (INFOCOM), pp. 2147-2155,Shanghai, China, 2011.