An Effective Approach for the Detection of Packet Dropping Attacks in MANETs

Pottapinjara Babu[1], Bhagavathy Thiraviam[2]

[1,2]*Assistant Professor, Department of Computer Science and Engineering*
[1,2]*Malla Reddy Engineering College (A), Hyderabad, Telangana, India.*

Abstract

Mobility and security location of Mobile Ad hoc Networks (MANET) is developed major domains. MANETs is commonly used network applications. Linkage error and small packet precede two sources for packet losses in mobile ad hoc network. A sequence of packet losses is present in the network. A distributed packet dropping attack (PDA) detection method is known as NAODV is proposed. Detection is small node is based on cooperative participation of many nodes' communication based on TRUST level. Conventional algorithm is used detecting packet loss rate and detection efficient the packet dropping rate is comparable to the channel error rate. The implement detection efficient correlations number of packets is finding. The packets are transmitted in the nodes with high trust value. Our experiment use NS2 with better performance. SAODV is detecting number of nodes identifying dropping of network and data packet. Packet dropping is link error and presence of small nodes is detected by SAODV. It also uses importance to security services of data and reduce the computation overhead a packet-block based on detection truthfulness for lower computation complexity. The proposed model is uses better detection and efficient to conventional methods.

Index Terms: *Wireless Ad-hoc Network, Public Auditing, Selective Dropping, Trust, Confidence, decision tree. Auditing, AES, homomorphism linear signature.*

1. Introduction

In a multi-hop wireless network, nodes get together in relay routing traffic. Associate someone will exploit this cooperative nature to launch attacks. For instance, the someone might 1st faux to be a cooperative node within the route discovery method. Once being enclosed in a very route; the someone starts dropping packets. Within the most severe type, the malicious node merely stops forwarding each packet received from upstream nodes, fully disrupting the trail between the supply and therefore the destination. Eventually, such a severe Denial-of Service (DoS) attack will paralyze the network by partitioning its topology. Even though persistent packet dropping will effectively degrade the performance of the network, from the attacker's viewpoint such associate "always-on" attack has its disadvantages. First, the continual presence of extraordinarily high packet loss rate at the malicious nodes makes this sort of attack simple to be detected .Second, once being detected, these attacks area unit simple to mitigate. for instance, just in case the attack is detected however the malicious nodes aren't known, one will use the irregular multi-path routing algorithms [8, 19] to circum-vent the black holes generated by the attack, probabilistically eliminating the attacker. Vulnerability is a weakness in security system. A system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Security is an essential service for wireless network communications. However, the characteristics of MANETS pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and no repudiation [3]. A user can continue to access and manipulate desired data while traveling on plane, in car, on ship, etc. Thus, the discipline creates an illusion that the desired data and sufficient processing power are available on the spot, whereas in reality they may be located far away. Wireless ad hoc networks are collections of wireless nodes, that communicate directly over common wireless

channel. The nodes are equipped with wireless transceiver. They don't need any additional infrastructure, such as base station or wired access point, etc. Therefore, each node doesn't only plays the role of an end system, but also acts as a router, that sends packets to desired nodes. The ad hoc are expected to do assignments, which the infrastructure can't do. Ad hoc networks are mostly used by military, rescue mission team, taxi drive.

Figure 1. Structure of mobile computing

2. Related Works

Based on how much weight a detection algorithm gives to link errors relative to malicious packet drops, the works had been done to detect the malicious packet dropping can be broadly classified into two. First category focuses on the detection with high malicious dropping rates, where the link errors are ignored. Based on the nature of the detection algorithm, this can be further classified into four. The first sub-category is based on credit systems [9].In this node gets incentive for its cooperation in transmission. When the node correctly transmits the packets to the next hop, it gets credit. Based on the credit value, the node gets priority during the transmission of its own packets. Thus, when the attacker continuously drops packets, its credit decreases and automatically gets expelled from the network. But when the attacker performs a selective dropping, it gets enough credits and can continue as a part of the network. The second subcategory is based on reputation systems [4-7]. In this mechanism the neighbour nodes monitor the activity of all nodes. For a node that drops packets maliciously gets a bad reputation. The reputation is the determining factor while selecting a route for transmission. Thus, malicious nodes get excluded from a route. In this mechanism also, if the attacker selectively drops packets and forward some packets, then it can have a better reputation. The second category of works focus on the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is no negligible. This type of mechanisms requires the knowledge of the wireless channel.

The works in [9, 10] proposed to detect malicious packet dropping by counting the number of lost packets. If the number of lost packets is significantly larger than the expected packet loss rate made by link errors, then with high probability a malicious node is contributing to packet losses. But counting the number of lost packets is not enough to detect the attacker. There are some unknown events, which cause access point's malfunction. The nodes lose their network and they are quasi not working. It is the biggest infrastructure's disadvantage. There are also some reasons to sacrifice or not to use access point's services. These can be cost factor, impossibility to install access point in short time, etc. In this case the nodes must build its own network. This network is called wireless ad hoc network. The wireless ad hoc networks only consist of nodes equipped with transceiver. The network is created to be independent from an infrastructure. Therefore, the nodes must be able to arrange their own networks. A node can now communicate only with other nodes in its transmission range. In the infrastructure based wireless network, the nodes can communicate with a node, which is in another network area, by transmitting data to destination access point and this access point relay the data to the desired node. It seems like, that the ad hoc networks are not powerful enough. Each node has its own transmission range, if these small transmission areas are combined, they will form a much bigger transmission area. The nodes transmit their data with single or multiple hopping techniques. Now a

suitable routing algorithm must be implemented, so the process of transmitting data will be more effective.

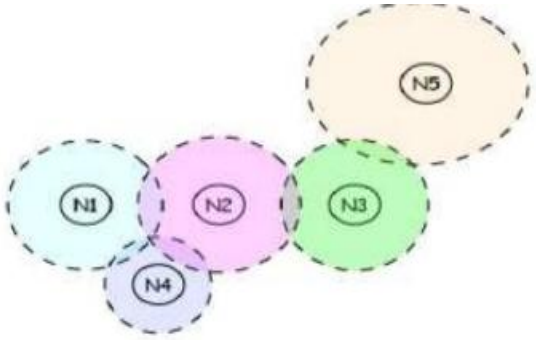


Figure 2. Transmission area in ad hoc

2. Secured Ad-hoc on-Demand Distance Vector Routing Protocol

In SAODV is proposed by adding additional security features to AODV. Which provides privacy for preserving truthful detection of packet dropping attack in MANET? Packet may be dropped during forwarding of routing information or during data forwarding. Dropping can be due to presents of malicious nodes or due to link error. SAODV can investigate the dropping and can find the malicious node or failed link behind this dropping. For identifying data packet dropping attack cryptographic scheme is added in SAODV. In this approach after identifying the source to destination path, all nodes included in the path should forward it's on public key to source node. Then the source node can encrypt the packet using public-key crypto-system such as RSA. Before the encryption process, the checksum value is calculated for the whole message. Message is then divided into packets. Each packet and its checksum are encrypted using RSA algorithm. Encryption is starting by using the public key of the destination node and end by the public key of nearest neighbour node of source. Checksum calculation is done by using MD5 algorithm [17].

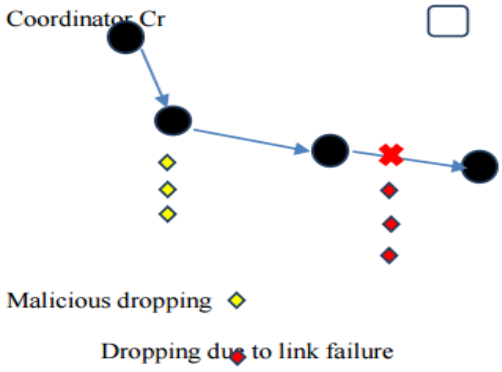


Figure 3. Network model

3. Proposed Methodology

In the system model, low rates of packet loss or any other packets drop other than malicious packet drop are assumed as threshold packet drop. When packet drop is more than the threshold packet drop than PDA is suspected. PDA is suspected in certain node based on the different network performance parameters such as packet delivery ratio as well as throughput of the network. It is assumed that packets are forwarded in a hop-by-hop fashion in on demand ad hoc way. The communication links are assumed to be bi-directional and there is no wireless channel error. All nodes use unidirectional antennas for bidirectional communications. Neighbor discovery protocol is assumed to be worked in such a way that every node can understand its corresponding neighbor. It is assumed that all the nodes in MANET have the capability to understand packet drop in them. Thus, it can understand the threshold packet drop as well as malicious packet drop. Promiscuous mode of node is enabled with

source routing. A malicious node can drop packets continuously or selectively. Here collusion of more than one node is not considered so that malicious node can monitor each other and collude and mask the misbehavior of each other We assume that intelligent agent is supposed to adapt decision making by the cooperation with other nodes in the communication. Activity of the agent is dependent on the network performance matrices such as:

- Delay in Delivery of the Packet.
- Response Time.
- Quality of Service Provider.
- Packet Forwarding Misbehavior

Proposed distributed PDA detection methodology is based on cooperation of different nodes. Data collected from different nodes are analyzed to detect PDA. Upon detection, message will be distributed amongst the nodes in terms of alarm to avoid the malicious nodes for packet forwarding. The entire system is an automatic, self manageable process. Data, collected from various nodes' host level audit system like "system log", are analyzed by the system. Then data abstraction is done on the collected data. As shown in Fig 1, different modules and their functions are discussed

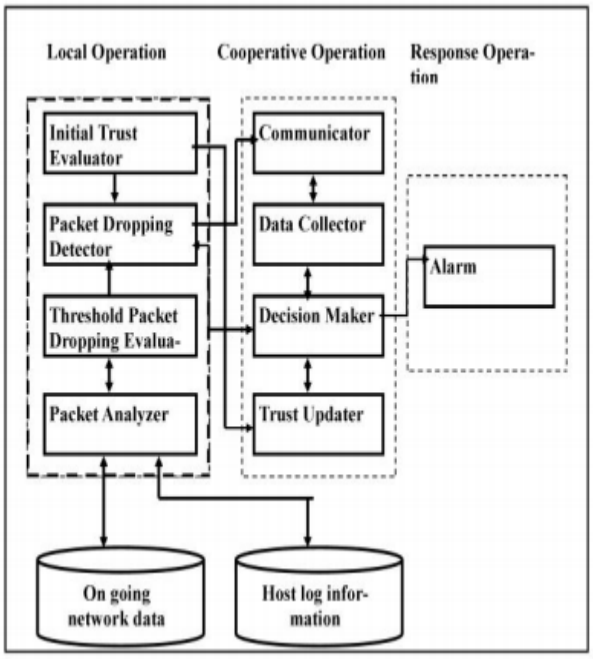


Figure 4. Schematic diagram of distributed PDA detection methodology

3.1. Proposed Detection Scheme

The proposed mechanism is based on detecting the correlations between the lost packets over each hop of the path. The basic idea is to model the packet loss process of a hop as a random process alternating between 0 (loss) and 1 (no loss). Specifically, consider that a sequence of M packets that are transmitted consecutively over a wireless channel. By observing whether the transmissions are successful or not To develop an accurate algorithm for detecting selective packet drops made by insider attackers. This algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap–a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions.

3.2. Network and Channel Models

Consider associate absolute path PSD in a very multi-hop wireless circumstantial network, as shown in Figure 4. The supply node S ceaselessly sends packets to the destination node D through intermediate nodes n1, . . . ,nK , wherever Ni is that the upstream node of ni+1, for one i K one. we tend to assume that S is alert to the route PSD, as in Dynamic supply Routing (DSR) [15]. If DSR isn't used, S will establish the nodes in PSD by playing a traceroute operation. Here we tend to in the main target visible once the quantity of maliciously born packets is comparable those caused by link errors. to properly calculate the correlation between lost packets, it's crucial to accumulate truthful packet-loss info at individual nodes. we tend to develop associate HLA-based public auditing design that ensures truthful packet-loss reportage by individual nodes. This design is collusion proof, needs comparatively high procedure capability at the supply node, however, incurs low communication and storage overheads over the route. to scale back the computation overhead of the baseline construction, a packet-block-based mechanism was conjointly projected, that permits one to trade detection accuracy for lower computation complexness.

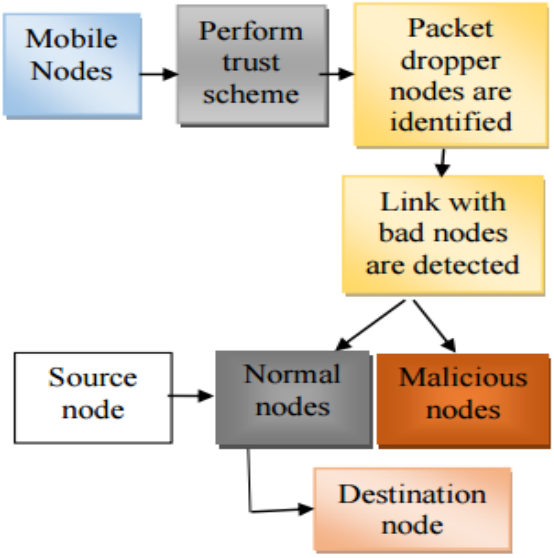


Figure 5. Block diagram of trust scheme

3.3. Audit Phase

This phase is triggered when the public auditor Ad receives an ADR message from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream direction, i.e., n1, . . . , nK , S's HLA public key information pk = (v, g, u), the sequence numbers of the most recent M packets sent by S, and the sequence numbers of the subset of these M packets that were received by D. Recall that we assume the information sent by S and D is truthful, because detecting attacks is in their interest. Ad conducts the auditing process. Note that the above mechanism only guarantees that a node cannot understate its packet loss, i.e., it cannot claim the reception of a packet that it actually did not receive. This mechanism cannot prevent a node from overly stating its packet loss by claiming that it did not receive a packet that it received. This latter case is prevented by another mechanism discussed in the detection phase.

Find_NextHopAddr(dstAddr)

Input: dstAddr – network address of the destination
Output: nextHopAddr - next hop address for the destination

1: Initialize minRouteCost with ∞
2: level(dstAddr), A(dstAddr) ←Find_Ancestors(dstAddr)
3: **for each** (neighbor's address n_k in neighbor table)
4: level(n_k), A(n_k) ←Find_Ancestors(n_k)
5: level(LCA) = 0
6: **while** (level(LCA) ≤ min(level(dstAddr), level(n_k)) and
A(dstAddr, level(LCA)) = A(n_k, level(LCA)))
7: ++ level(LCA)
8: **end while**
9: nbrRouteCost ←level(dstAddr) + level(n_k) – 2·level(LCA)
10: **if** (nbrRouteCost < minRouteCost)
11: nextHopAddr ← n_k
12: minRouteCost ← nbrRouteCost
13: **end if**
14: **end for each**
15: Transmit packet to nextHopAddr

3.4. Detection Phase

The public auditor Ad enters the detection phase after receiving and auditing the reply to its challenge from all nodes on PSD. The main tasks of Ad in this phase include the following: detecting any overstatement of packet loss at each node, constructing a packet-loss bitmap for each hop, calculating the autocorrelation function for the packet loss on each hop, and deciding whether malicious behavior is present. More specifically, Ad performs these tasks as follows. The auditor calculates the autocorrelation function. The detection process applies to one end-to-end path. The detection for multiple paths can be performed as multiple independent detections, one for each path. Although the optimal error threshold that minimizes the detection error is still an open problem, our simulations show that through trial-and-error, one can easily find a good ϵth that provides a better detection accuracy than the optimal detection scheme that utilizes only the pad of the number of lost packets.

4. Performance Evaluation

For comparing performance of AODV and SAODV ONE simulator is used. It is a java-based simulation tool. Main focus is truthful detection of packet dropping attack. Two separate MANET is created for this purpose and one is simulated with AODV and another with SAODV. From this experiment it is identified that routing complexity of SAODV is higher than AODV, but proper detection of packet dropping attack can done by SAODV. As Compared to AODV, SAODV have very high detection rate. Experiment also shows that SAODV truthfully detect packet dropping attack in MANET.

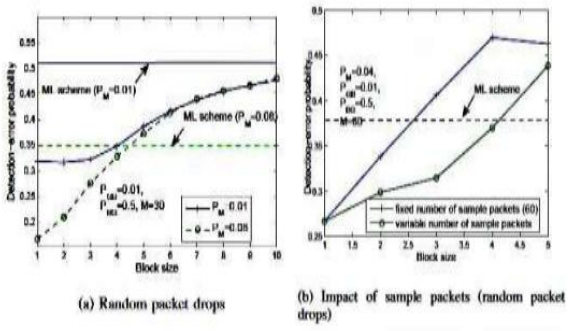
Simulation Setup: The detection accuracy which can be achieved by the Conventional algorithm with the optimal maximum likelihood algorithm that utilizes the distribution of the number of lost packets. For given packet-loss bitmaps, the detection on different hops is conducted separately. So, only need to simulate the detection of one hop to evaluate the performance of a given algorithm.

Selective Packet Dropping: The detection error as a function of the number of maliciously dropped packets. Similar performance trends can be observed to the case of the random packet dropping. Fewer detection errors are made by both algorithms when more packets are maliciously dropped. In all the simulated cases, the proposed algorithm can detect the actual cause of the packet drop more accurately than the ML scheme.

Dropping of Control Packets: The simulations so far have not made any application semantic (use case) assumption on the dropped packets. In reality, however, because these packets are usually used for control purposes, the loss of these packets may generate significant impacts on the

transmission of other (i.e., data) packets. In this series of simulations, to evaluate how the correlation between the control and data packets affects the performance of the proposed scheme.

Block-Based Detection: In this series of simulations, the detection accuracy of block-based algorithms as a function of block size In general, it shows that for both cases the detection error increases with the block size. This is expected, as a larger block size hides more details of packet losses, and therefore makes the actual correlation of lost packets more difficult to calculate. Meanwhile, the benefits of blocked-based algorithm is also observed. It is able to trade computation complexity for better detection accuracy



(a) Random packet drops (b) Impact of sample packets (random packet drops)

Figure 5. Detection accuracy of block-based algorithms

5. Conclusion

An accurate method for detecting selective packet drops made by insider attackers is proposed in this paper. It also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. Mobile Ad hoc Network (MANET) is a type of Ad-hoc Network which changes its location dynamically and configures itself. MANET does not have a fixed topology which causes priorities to different kind of attacks. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap–a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions. The proposed methodology has been experimented in various networks settings with various parameters. The respective results are compared with two existing systems and analyzed. This methodology doesn't consider the collaborative malicious packet dropping attack and battery power consumption. Moreover, condition of "No response" are not analyzed. The implementation and optimization of the proposed mechanism under various particular protocols will be considered in future studies.

6. Further Work

As a future enhancement this work can be extended to detect the selfish nodes which are malicious and malicious nodes which are acting as selfish nodes. The algorithm takes into account the cross statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets It is compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops.

References

[1] J. N. Arauz, "802.11 Markov channel modeling," Ph.D. dissertation, School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004

[2] B. Awerbuch, R. Curtmola, D.Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform.Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[3] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[4] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle. Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs, In Proc. of the 33rd IEEE Conference on Local ComputerNetworks (LCN), Dublin, Ireland, October 2007.

[5] W. Yu, Y. Sun and K. R. Liu, HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks, In Proc. 24th IEEE INFOCOM, Miami, USA, March 2005.

[6] Hayajneh.T, Krishnamurthy.P, Tipper.D, and Kim.T, "Detecting malicious packet dropping in the presence of collisions and channelerrors in wireless ad hoc networks" (2009).

[7] Kozma Jr.W and Lazos.L "REAct: resource-efficient accountabilityfor node misbehavior in ad hoc networks based on random audits". Wireless Network Security, (2009)

[8] Liu.K, Deng.J, Varshney.P, and Balakrishnan.K "An acknowledgement-based approach for the detection of routing misbehavior in MANETs". Vol. 6, no.5, pp.536–550, May 2006

[9] Malhotra. A, Kirtani. S , Agarwal.T "Detection of malicious route in wireless adhoc networks" PP. 1-4, Mar 2010.

[10] Ateniese.C, Burns.R, Curtmola.R, Herring.J, Kissner.L, Peterson.Z, and Song.D, "Provable data possession at untrusted stores"., pages 598–610, Oct. 2007.

[11] Julian Benadit.P, Sharmila Baskaran and Ramya Taimanessamy, "Detecting Malicious Packet Dropping Using Statistical Traffic Patterns", IJCSI International Journal of Computer Science Issues(2011), Vol.8, Issue 3, No. 2, ISSN (Online): 1694-0814

[12] V. Madhu Viswanatham and A.A. Chari, "An Approach for Detecting Attacks in Mobile Adhoc Networks", Journal of Computer Science 2008, Volume 4, Issue 3, Pages 245-251

[13] Ricardo Puttini, Jean-Marc Percher, Ludovic Mé and Rafael de Sousa, "A Fully Distributed IDS for MANET", Computers and Communications, 2004. Proceedings. ISCC 2004. Vol. 1, Page(s): 331 – 338, Print ISBN: 0-7803-8623- X

[14] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks. Chapter 5, Ad Hoc Networking, Addison-Wesley, pages 139–172, 2001..

[15] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the ACM MobiHoc Conference, pages 46–57, 2005.

[16] A. Proano and L. Lazos. Selective jamming attacks in wireless networks. In Proceedings of the IEEE ICC Conference, pages 1–6, 2010.

[17] W. Kozma Jr. and L. Lazos. REAct: resource-efficient answerability for node misconduct in circumstantial networks supported random audits. In Proceedings of the ACM Conference on Wireless Network Security (WiSec), 2009.

[18] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan. associate acknowledgement-based approach for the detection of routing misbehav-ior in MANETs. IEEE Transactions on Mobile Computing, 6(5):536– 550, May 2006.

[19] Y. Liu and Y. R. Yang. name propagation and agreement in mobile ad-hoc networks. In Proceedings of the IEEE WCNC Conference, pages 1510–1515, 2003.

[20] G. Ateniese, S. Kamara, and J. Katz, ―Proofs of storage from homomorphic identification protocols,‖ in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319– 333.

[21] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, ―ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks,‖ ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

[22] K. Balakrishnan, J. Deng, and P. K. Varshney, ―TWOACK: Preventing selfishness in mobile ad hoc networks,‖ in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[23] D. Boneh, B. Lynn, and H. Shacham, ―Short signatures from the weil pairing,‖ J. Cryptol., vol. 17, no. 4, pp. 297– 319, Sep. 2004.