International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-5)

Research Article

May
2014

A Secure Selective Jamming Technique against Malicious Agent Using DSA Algorithm

P.Balasubramani
PG Student
Computer Science & Engineering
PSNA College of Engineering and Technology , India

N. Uma Maheswari
Professor
Computer Science & Engineering
PSNA College of Engineering and Technology, India

Abstract—

A wireless sensor networks (WSNs) pledge many new enthuse applications in the future, as ubiquitously on-demand multiply ascendancy, continual connectivity, and instantaneously deployable communication for armed and responders. These types of wireless sensor networks already help to observe critical environmental conditions in volcanic eruption areas, underwater and so on; factories maintenance works, and troop utilization, to name a few applications. As WSNs grow to be a greater extent essential to the everyday performance of people and organizations and also many attacks are arisen in the wireless as hoc networks. The wireless intermediate is constantly subjected to deliberate intervention attacks in the networks such as jamming attacks. These types of selective congestion attacks in the WSN can be tattered for increasing DOS assaults. In order to overcome to disadvantages in the previously proposed schemes, we proposed the new approach to prevent the selective jamming attacks in the WSN. In the proposed system, we introduce a Self-Organizing Trust model (SORT) that aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity. No a priori information or a trusted peer is used to leverage trust establishment. Peers do not try to collect trust information from all peers. Each peer develops its own local view of trust about the peers interacted in the past. In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers. Since peers generally tend to interact with a small set of peers forming trust relations in proximity of peers helps to mitigate attacks in a P2P system. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

Keywords— Jammer, DOS, Probing Technique, Spread Spectrum, Pseudonoise, data hiding, jamming signals, Strong hiding commitment scheme

I. INTRODUCTION

Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. This paper presents distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions and recommendations. Peers create their own trust network in their proximity by using local information available and do not try to learn global trust information. Two contexts of trust, service, and recommendation contexts are defined to measure trustworthiness in providing services and giving recommendations. Interactions and recommendations are evaluated based on importance, recentness, and peer satisfaction parameters. Additionally, recommender's trustworthiness and confidence about a recommendation are considered while evaluating recommendations. Simulation experiments on a file sharing application show that the proposed model can mitigate attacks on 16 different malicious behavior models. In the experiments, good peers were able to form trust relationships in their proximity and isolate malicious peers.

We also find that, in a scenario where the intermediate nodes gather as a close cluster, the cooperative jamming schemes may be less effective than their non-jamming counterparts. Therefore, we introduce a hybrid scheme to switch between jamming and non-jamming modes. Simulation results validate our theoretical analysis that the hybrid switching scheme further improves the secrecy rate.

A Wireless ad hoc wireless sensor networks (WSNs) assuring many new exciting applications in the future, such an everywhere on-demand computing supremacy, incessant connectivity, and instantaneously deployable communication for armed and responders. As WSNs grow to be a greater extent essential to the everyday performance of people and organizations and also many attacks are arisen in the wireless as hoc networks. The authors proposed many systems to address the selective jamming attacks in the WSN and so the author proposed predictable anti-jamming performance rely expansively on spread-spectrum (SS) relations, or some appearance of congestion avoidance in the WSN. Spread Spectrum technique in the wireless communication system afford bit-level fortification by scattering crumbs according to a furtive pseudo-noise (PN) system, identified only to the corresponding communication parties in WSN. Transmit communications are predominantly defenceless under a domestic menace model because all predictable recipient must be awake of the secret information or data used to protect communication. We believe a difficult adversary or attacker who is responsive of system undisclosed and the execution details of system protocols at several layers in the system stack of the networks. Author's proposed a resolution based on all – Or - Nothing renovation (AONR) that introduces a modest communication and computation overhead. An AONR provides as an overtly known and entirely invertible pre-processing step to a plaintext before it is passed to an ordinary encryption algorithm.

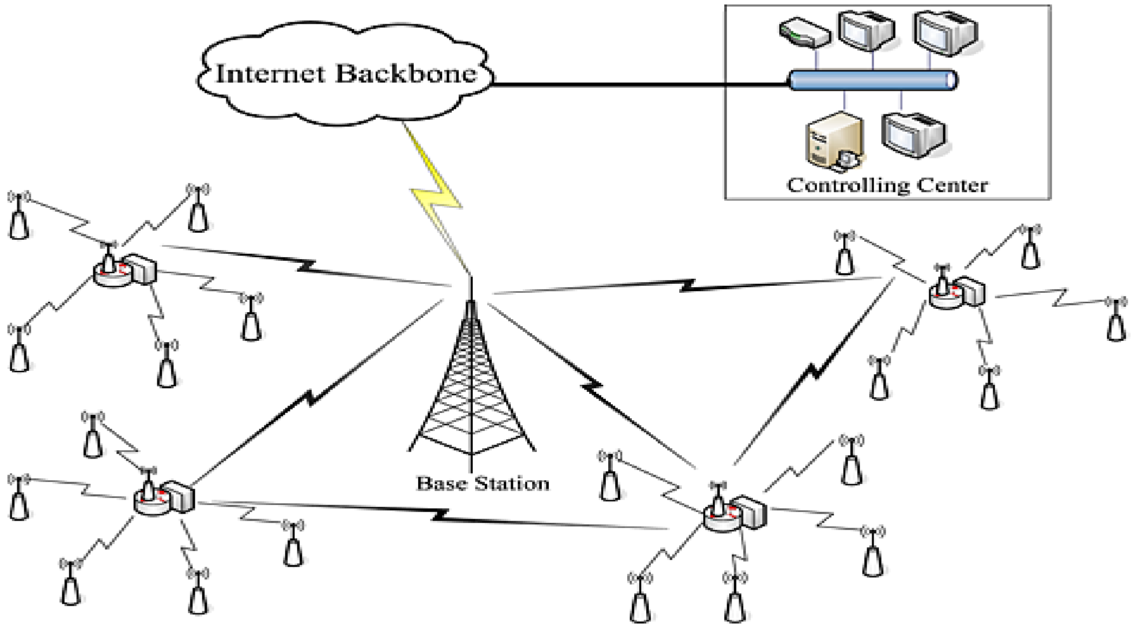


Figure 1: Typical Model for Jamming Attacks in WSN

In the previous system, some selective jamming happens in the networks so to address this we proposed the new approach in this paper. We propose a secure selective jamming technique with the use of DSA algorithm. Router acts as a relay R and monitoring the data flow. After select the data in server it split into several packets. In each pocket assign a signature. Each client is connected with respective IP address. In normal P2P systems peer send the information to client, in that technique it can able to send with in this group and within the configuration. To overcome the configuration and transformation problem, here apply a selective jamming technique. Relay node R monitor the data flow and it can manage the huge traffic . In cause the traffic (queue) length get increasing mean the data flow pause by relay node. Then when the queue size get free the retransmission is possible and no need to send the full data. It automatically send the data from when it got stop. Algorithm identifies every node which is receptive for the succeeding node. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.The rest of the paper will be organised as follows: In section 2, we see about the related works of the paper. In section 3, we discuss about the proposed method. The algorithms and simulation are shown in the section 4 and 5. The conclusion of our paper is in section 6.

II. RELATED WORKS

In this section, we will see the some of the literature review of using different approaches:

“Claude Cr´epeau, Carlton R. Davis∗ and Muthucumaru Maheswaran School of Computer Science, McGill University,.

To overcome byzantine behavior (loss of data) robust secure routing (RSR) protocol are used. It providing data origin authentication services and integrity check’s. RSR protocol is able to mitigate against intelligent malicious agents which selectively drop or modify packets they agreed to forward. In addition to providing data origin authentication services and integrity checks, RSR is able to mitigate against intelligent malicious agents which selectively drop or modify packets they agreed to forward.

Due [2] to their very nature, wireless sensor networks are probably the category of wireless networks most vulnerable to "radio channel jamming"-based denial-of-service (DoS) attacks. An adversary can easily mask the events that the sensor network should detect by stealthily jamming an appropriate subset of the nodes; in this way, he prevents them from reporting what they are sensing to the network operator. Therefore, even if an event is sensed by one or several nodes (and the sensor network is otherwise fully connected), the network operator cannot be informed on time. We show how the sensor nodes can exploit channel diversity in order to create wormholes that lead out of the jammed region, through which an alarm can be transmitted to the network operator. We propose three solutions. The first is based on wired pairs of sensors, the second relies on frequency hopping, and the third is based on a novel concept called uncoordinated channel hopping. We develop appropriate mathematical models to study the proposed solutions

In this paper [3], we address the problem of countering jamming of broadcast control channels in wireless communication systems. Targeting control traffic on a system, e.g., BCCH channel in GSM, leads to smart attacks that can be four orders of magnitude more efficient than blind jamming. We propose several schemes based on coding theory and its applications that can counter both external and internal attackers (traitors). We introduce a T-(traitor) resilient scheme that requires less than (T logT N)2 control information transmissions and guarantees delivery of control information against any coalition of T traitors. The proposed scheme also allows the identification of persistently jamming traitors.

Wireless ad hoc networks [4] have fundamentally altered today's battlefield, with applications ranging from unmanned air vehicles to randomly deployed sensor networks. Security and vulnerabilities in wireless ad hoc networks have been considered at different layers, and many attack strategies have been proposed, including denial of service (DoS) through the intelligent jamming of the most critical packet types of flows in a network. This investigates the effectiveness of intelligent jamming in wireless ad hoc networks using the Dynamic Source Routing (DSR) and TCP protocols and introduces an intelligent classifier to facilitate the jamming of such networks. Assuming encrypted packet headers and contents, our classifier is based solely on the observable characteristics of size, inter-arrival timing, and direction and classifies packets with up to "9.4% accuracy in our experiments.

We present the design [5] and evaluation of an 802.11-like wireless link layer protocol that obfuscates all transmitted bits to increase privacy. This includes explicit identifiers such as MAC addresses, the contents of management messages, and other protocol fields that the existing 802.11 protocol relies on to be sent in the clear. By obscuring these fields, we greatly increase the difficulty of identifying or profiling users from their transmissions in ways that are otherwise straightforward. Our design, called SlyFi, is nearly as efficient as existing schemes such as WPA for discovery, link setup, and data delivery despite its heightened protections; transmission requires only symmetric key encryption and reception requires a table lookup followed by symmetric key decryption. Experiments using our implementation on Atheros 802.11 drivers show that SlyFi can discover and associate with networks faster than 802.11 using WPA-PSK. The overhead SlyFi introduces in packet delivery is only slightly higher than that added by WPA-CCMP encryption (10% vs. 3% decrease in throughput).

Conventional methods for mitigating jamming employ some form of SS communications [5]. The transmitted signal is spread to a larger bandwidth following a PN sequence. Without the knowledge of this sequence, a large amount of energy (typically 20-30 dB gain) is required to interfere with an ongoing transmission. However, in the case of broadcast communications, compromise of commonly shared PN codes neutralizes the advantages of SS. Popper et al. proposed a jamming-resistant communication model for pairwise communications that does not rely on shared secrets. Communicating nodes use a physical layer modulation method called Uncoordinated Direct-Sequence Spread Spectrum (UDSSS) [2]. They also proposed a jamming-resistant broadcast method in which transmissions are spread according to PN codes randomly selected from a public codebook [2]. Several other schemes eliminate overall the need for secret PN codes [5], [2]. Lin and Noubir showed that jamming 13 percent of a packet is sufficient to overcome the ECC capabilities of the receiver [3]. Xu et al. [7] categorized jammers into four models: 1. a constant jammer, 2. a deceptive jammer that broadcasts fabricated messages, 3. a random jammer, and 4. a reactive jammer that jams only if activity is sensed [3]. They further studied the problem of detecting the presence of jammers by measuring performance metrics such as packet delivery ratio [8], [9], [10]. Cagalj et al. proposed wormhole-based anti jamming techniques for wireless sensor networks [2]. Using a wormhole link, sensors within the jammed region establish communications with outside nodes, and notify them regarding ongoing jamming attacks.

III. **PROPOSED WORK**

In the previous system, some selective jamming happens in the networks so to address this we proposed the new approach in this paper. We propose a secure selective jamming technique with the use of DSA algorithm. Router acts as a relay R and monitoring the data flow. After select the data in server it split into several packets. In each pocket assign a signature. Each client is connected with respective IP address. In normal P2P systems peer send the information to client, in that technique it can able to send with in this group and within the configuration. To overcome the configuration and transformation problem, here apply a selective jamming technique. Relay node R monitor the data flow and it can manage the huge traffic . In cause the traffic (queue) length get increasing mean the data flow pause by relay node. Then when the queue size get free the retransmission is possible and no need to send the full data. It automatically send the data from when it got stop. Algorithm identifies every node which is receptive for the succeeding node. In the proposed system, we introduce a Self-Organizing Trust model (SORT) that aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity. No a priori information or a trusted peer is used to leverage trust establishment. Peers do not try to collect trust information from all peers. Each peer develops its own local view of trust about the peers interacted in the past. In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers. Since peers generally tend to interact with a small set of peers forming trust relations in proximity of peers helps to mitigate attacks in a P2P system. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

IV. ALGORITHM

Digital signature Algorithms are used to provide authentication of data, and validating the sender.

- Public key signature schemes.
- The private-key signs (creates) signatures.
- The public-key verifies signatures.
- Only the owner (of the private-key) can create the digital signature. Hence it can be used to verify who created a message. Anyone knowing the public key can verify the signature providing they are confident of the identity of the owner of the public key.
- The key distribution problem usually don’t sign the whole message Since this would double the amount of information exchanged.

Digital signatures can provide non-repudiation of message origin, since an asymmetric algorithm is used in their creation, provided suitable timestamps and redundancies are incorporated in the signature.

DSA KEY GENERATION

Firstly shared global public key values (p,q,g) are chosen ;

- Choose a large prime p = 2^L
  Where L = 512 to 1024 bits and is a multiple of 64
- Choose q , a 160 bit prime factor of p-1
- Choose g = h ^ (p-1)/q
  For any h,p-1, h^(p-1)/q (mod p)>1
- Then each user chooses a private key and computes their public key ;
- Choose x<q
- Compute y = g^x (mod p)

DSA SECURITY

- Basic security rests on difficulty of computing discrete logarithms mod p.Original recommendation was to use a common modules p-a tempting target
- Now recommended different group choose own public parameters (p,q,g)
- Possible to do both ELGamal and RSA encryption using DSA routines, which was not intended.
- DSA is patented with royalty free use, but this patent has been contested , situation unclear Gus Simmons has found a subliminal channel in DSA , could be used to leak the private key from a library make sure your library implementer.Security of DSA is regarded as high (basically as good as RSA ELGmal with same size modulus), but it’s more efficient. hence it’s not a popular choice.

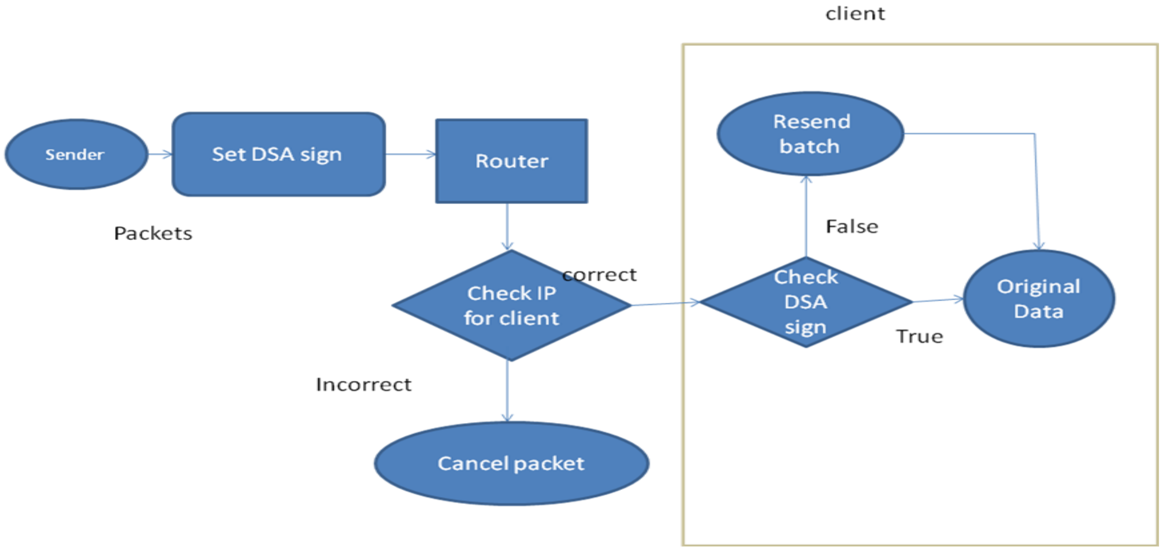
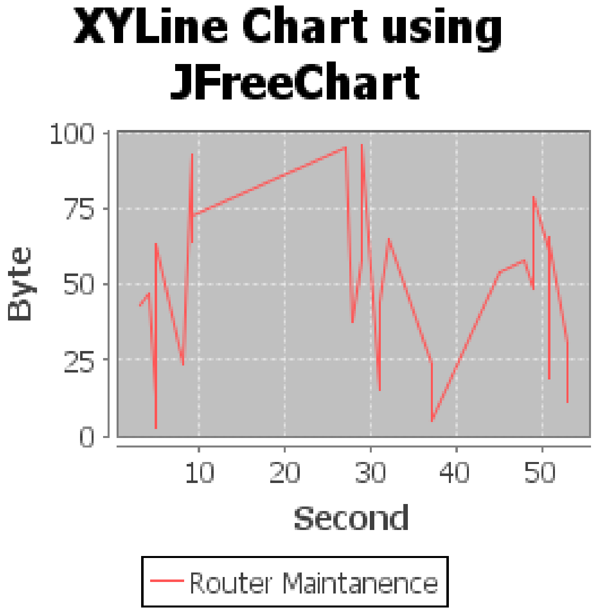


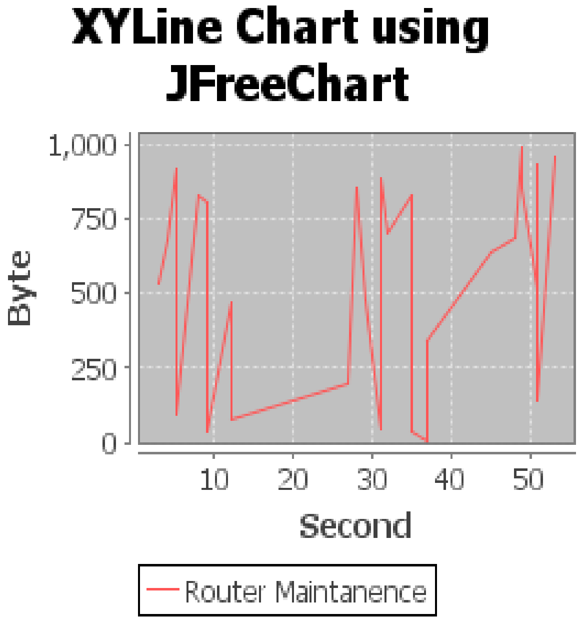
Figure.2. Proposed secure selective jamming System with the use of DSA

V. SIMULATION WORKS/RESULTS

Implementation is the process of converting a new or revised system design into an operational one. The implementation is the final and important phase. It involves ser training, system testing and successfully running of developed proposed system. The user tests the developed system and changes are made according to their needs. The testing phase involves the testing of developed system using various kinds of data.

An elaborate testing of data is prepared and the system is tested using that test data. The corrections are also noted for future use. The users are trained to operate the developed system. Both the hardware and software securities are made to run the developed system successfully in future.





Two ways Co-Operative Network

In this module, we can implement information exchange against eavesdroppers in two-way cooperative networks, consisting of two sources, one eavesdropper, and a number of intermediate nodes, with secrecy constraints. Specifically, an intermediate node is selected to operate in the conventional amplify-and-forward (AF) relay mode and assists the sources to deliver data to the corresponding destinations. Meanwhile, another two intermediate nodes that perform as jamming nodes are selected and transmit artificial interference in order to degrade the eavesdropper links in the first and second phase of data transmission, respectively

Conventional selection without jamming

In this module, in a conventional cooperative network, the relay scheme does not have a jamming process. The conventional selection does not take the eavesdropper channels into account and the relay node is selected according to the instantaneous signal - to- noise ratio (SNR) of the links between Source 1 to Source 2.

Simulation Results

The intermediate nodes spread randomly within the square space. It is clear that selection with jamming outperform their non-jamming counterparts within a certain transmitted power range. Outside this range the secrecy rate of OSJ converges to a power-independent value. Whereas the ergodic secrecy rate of OS continues to grow with a slope. This validates the analysis the suboptimal scheme SSJ performs almost the same as the optimal scheme OSJ. Furthermore, it can be seen from that OW provides better performance than any other selection techniques with or without continuous jamming. Within this configuration, we also compare the performance of different selection techniques measured by secrecy outage probability.

VI. Conclusion

It is the process of sending data from server to client via router. The router monitors the entire data transfer and data flow from the client from server. And also the data transfer take place for a particular client. To avoid unauthorised access of data it adds the DSA signature with the data. If the traffic increased in the router side it pause the process and finish the pending process then continue with the newly arriving process.

The proposed schemes achieve an opportunistic selection of one conventional relay node and one (or two) jamming nodes to enhance security against eavesdroppers based on both instantaneous and average knowledge of the eavesdropper channels. The selected relay node helps the information transmission between the two sources in an AF strategy, while the jamming nodes are used to produce intentional interference at the eavesdropper in different transmission phases.

References

[1] "A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes" Claude Cr´epeau, Carlton R. Davis∗ and Muthucumaru Maheswaran School of Computer Science, McGill University, Montr´eal, QC, Canada H3A2A7 IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 40, NO. 1, JANUARY 2007.

[2] "Cross-Layer Interaction of TCP and Ad Hoc Routing Protocols in Multihop IEEE 802.11 Networks" Kitae Nahm, Member, IEEE, Ahmed Helmy, Member, IEEE, and C.-C. Jay Kuo, Fellow, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 4, APRIL 2008.

[3] "Context-Aware Migratory Services in Ad Hoc Networks" Riva, O. Helsinki Inst. for Inf. Technol., Helsinki,, Nadeem, T. ; Borcea, C. ; Iftode, L. student member in IEEE TRANSACTIONS ON mobile computing, VOL. 6, NO3 DEC 2007.

[4] "Effective and Efficient Jamming Based on Routing in Wireless Ad Hoc Networks" jae-joon lee jangwee res. Inst . for Nat. Defence, Ajou Univ., Suwon, South Korea Jaesung Lim , Member, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, NOVEMBER 2012.

[5] "Joint Relay and Jammer Selection for Secure Two-Way Relay Networks" Jingchao Chen, Rongqing Zhang, Student Member, IEEE, Lingyang Song, Member, IEEE,Zhu Han, Senior Member, IEEE, and Bingli Jiao, Member, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.

[6] "Intelligent sensing and classification in ad hoc networks" Dempsey, T. Miami University Sahin, G. ; Morton, Y.T. ; Hopper, C.M. senior member IEEE TRANSACTIONS ON Aerospace and Electronic Systems Magazine, IEEE (Volume:24 , Issue: 8) AUG 2009

[7] "Mitigating the effect of jamming signals in wireless ad hoc and sensor networks" Sarker j.h ,mouftha t.h Sch. of Inf. Technol. & Eng. (SITE), Univ. of Ottawa, Ottawa, ON, Canada Member, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.

[8] "SORT: A Self-ORganizing Trust Model for Peer-to-Peer System" Ahmet Burak Can, Member, IEEE, and Bharat Bhargava, Fellow, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 1, JANUARY/FEBRUARY 2013.

[9] "TRECON: A Trust-Based Economic Frameworkfor Efficient Internet Routing" Zhengqiang Liang and Weisong Shi, Senior Member, IEEE IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 40, NO. 1, JANUARY 2010.

[10] "Traffic Policing over Various Ad Hoc Networks and Inter-Vehicular Communications" prahmkaew.s Senior Member, IEEE IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 40, NO. 1, AUG 2010.