Detecting Link Error and Malicious Packet Dropping Attacks using Homomorphic Linear Authenticator (HLA) in Wireless Ad-hoc Network

Dr. T. Ramaprabha[1], M.karthika[2]
Professor[1], M.Phil Full Time Research Scholar[2],
Department of Computer Science & Applications[1], [2]
Vivekanandha College of Arts and Sciences for Women (Autonomous), Namakkal, TamilNadu, India.
E-mail id: jpkarthika3@gmail.com,ramaradha1971@gmail.com

Abstract: **Link error and malicious packet dropping are two sources for packet losses in wireless ad hoc network. While observing a sequence of packet losses in the network, we are interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious packet drop.. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to exploit the correlations between lost packets. In this paper We develop a Homomorphic Linear Authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed.**

Keywords: **Wireless Adhoc Network (WANET), Packet dropping, secure routing, attack detection, Homomorphic Linear Authenticator (HLA), public auditing.**

1. I. INTRODUCTION

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, an ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks. It also refers to a network device's ability to maintain link status information for any number of devices in a 1 link (aka "hop") range, and thus this is most often a Layer 2 activity. Because this is only a Layer 2 activity, ad hoc networks alone may not support a routable IP network environment without additional Layer 2 or Layer 3 capabilities.

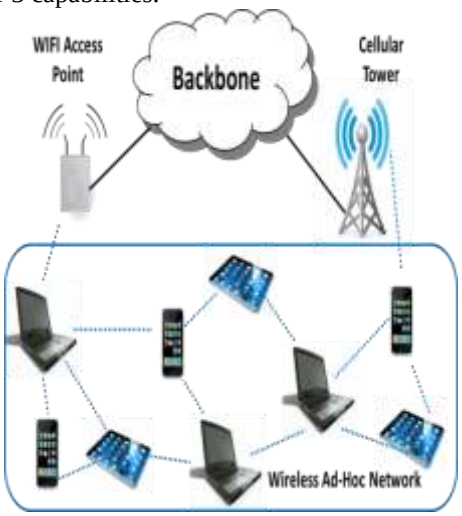


Figure 1: Wireless ad-hoc network

In spite of existing 802.11security techniques including Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), or 802.11i (WPA2), such methodology can only protect data frames—an attacker can still spoof management or control frames to cause significant impact on networks. Spoofing attacks can further facilitate a variety of traffic injection attacks, such as attacks on access control lists, rogue access point (AP) attacks, and eventually Denial-of- Service (DoS) attacks.

2. II. METHODOLOGY

Methodology is the systematic, theoretical analysis of the methods applied to a field of study. It comprises the theoretical analysis of the body of

methods and principles associated with a branch of knowledge. Typically, it encompasses concepts such as paradigm, theoretical model, phases and quantitative or qualitative techniques. A methodology does not set out to provide solutions - it is, therefore, not the same as a method. Instead, a methodology offers the theoretical underpinning for understanding which method, set of methods, or so-called "best practices" can be applied to specific case, for example, to calculating a specific result. It has been defined also as follows:

1. "The analysis of the principles of methods, rules, and postulates employed by a discipline";
2. "The systematic study of methods that are, can be, or have been applied within a discipline";
3. "The study or description of methods".
    - Attackers Modules.
    - Homomorphic Encryption Functions.
    - Threat models.
    - Enhanced Privacy against traffic analysis and flow tracing.
    - Security Analysis.

A. ATTACKERS MODULES

The appearance of an endangered monster (Attackers) in a monitored area is survived by wireless sensor, at the each time the inside and outside sensors are sensing to find out the attackers location and the timing. This information is passed to the server for analyzing. After analyzing the commander and Hunter they are also can participate this wireless network. In the commander and hunter itself some intruders are there, our aim to capture the attackers before attempting the network.

B. HOMOMORPHIC ENCRYPTION FUNCTIONS

We used the homomorphic encryption function is highly efficiency and securable. In the Commander process, we using this for each packet encryption .Due to the Homomorphism of HEFs, message recoding at intermediate nodes can be directly performed on encrypted and encoded messages, without knowing the decryption keys or performing expensive packet.

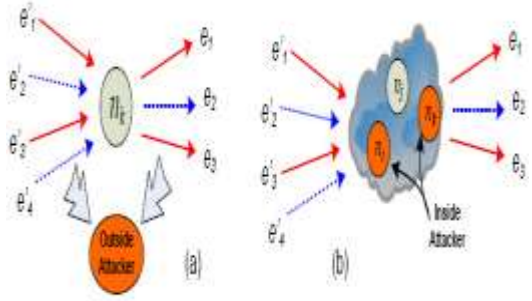
The performance evaluation on computational complexity demonstrates the efficiency of the proposed scheme. Homomorphic Encryption Functions (HEFs) have the property of homomorphism, which means operations on plaintext can be performed by operating on corresponding cipher text.

C. THREAT MODELS

We consider the following two attack models.

Outside Attacker: An outside attacker can be considered as a global passive eavesdropper who has the ability to observe all network links, as shown in Fig. 2 An outside attacker can examine the tags and message content, and thus link outgoing packets with incoming packets. Further, even if end-to-end encryption is applied to messages at a higher layer, it is still possible for a global outside attacker to trace packets by analyzing and comparing the message cipher text.

Inside attacker: An inside attacker may compromise several intermediate nodes, as shown in Fig.2 Link-to -link encryption is vulnerable to inside attackers since they may already have obtained the decryption keys and thus the message plaintext can be easily recovered. Both inside and outside attackers



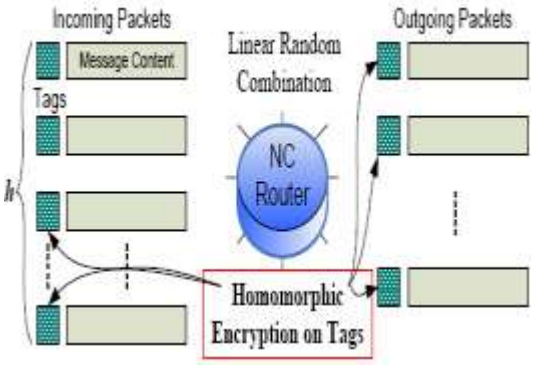
may perform more advanced traffic analysis/flow tracing techniques, including size correlation, time correlation, and message content correlation.

Figure 2: Finding Attacker

D. ENHANCED PRIVACY AGAINST TRAFFIC ANALYSIS AND FLOW TRACING

With the employment of HEFs, the confidentiality of GEVs is effectively guaranteed, making it difficult for attackers to recover the plaintext. Unlike other packet-forwarding systems,

Figure 3: Homomorphic Encryption



network coding allows intermediate nodes to perform computation on incoming messages, making outgoing messages be the mixture of incoming ones.

Flow tracing in the sense of the report about the alerting sensor.

E. SECURITY ANALYSIS

The generation number of a packet can be hidden in the secure routing scheme through link-to-link encryption. In this way, attackers cannot find the generation number of a packet for their further analysis. Notice that secure routing paths are only required to be established at the beginning of each session; during the packet transmission, secure routing paths are not required to change or re-established for each new generation.

3. IV. EXPERIMENTS AND RESULTS

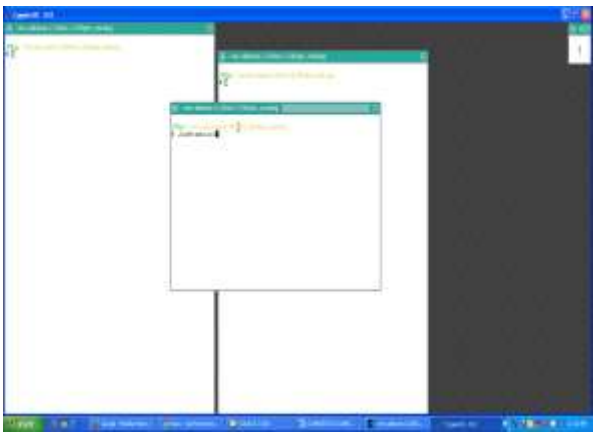


Fig4.1: NETWORK SIMULATOR WINDOW

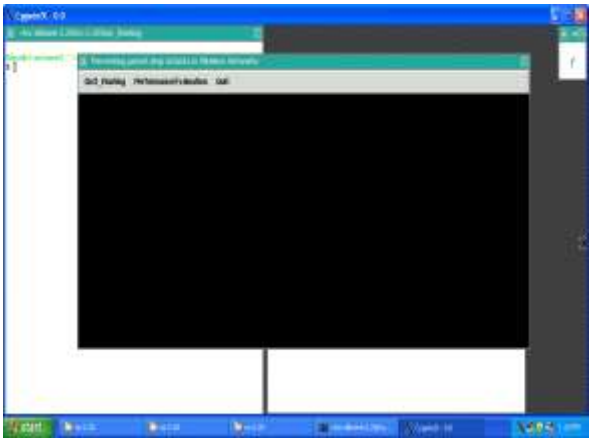


Fig 4.2: ROUTING PROCESS

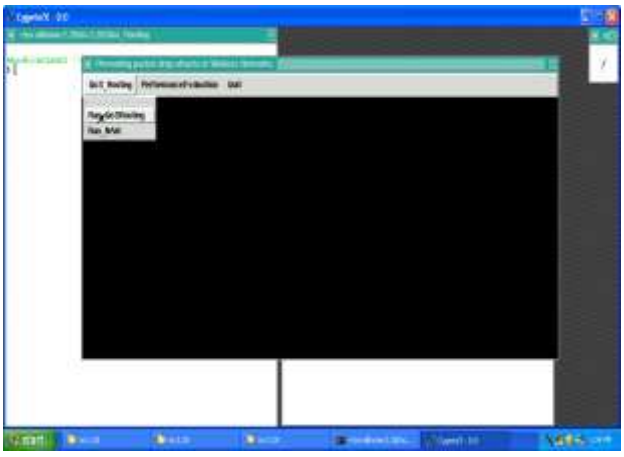


Fig 4.3: RUN ROUTING PROCESS

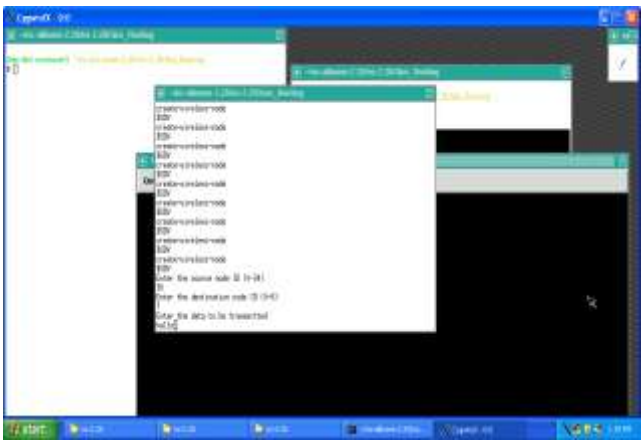


Fig 4.4: ENTER SOURCE AND DESTINATION

We consider 35 nodes. Here we have to enter the source node, destination node and enter the data which is to be transfer.

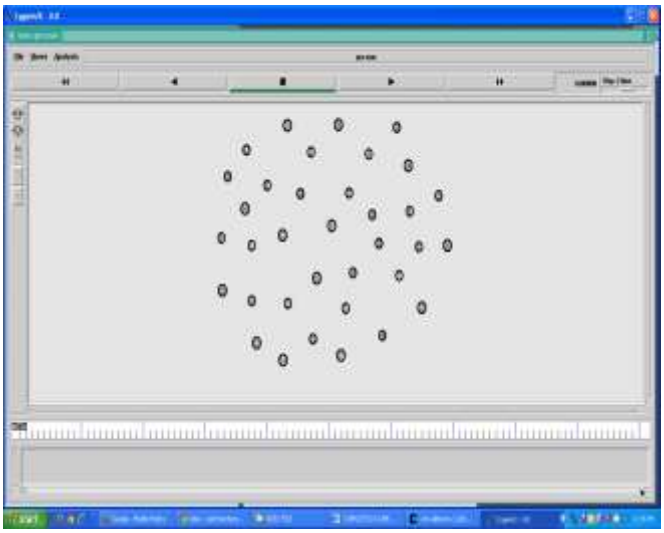


Fig4.5: NODE ARRANGEMENT

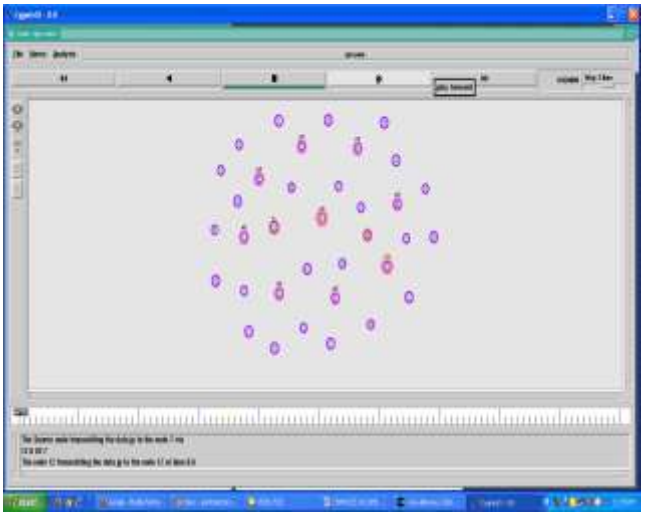
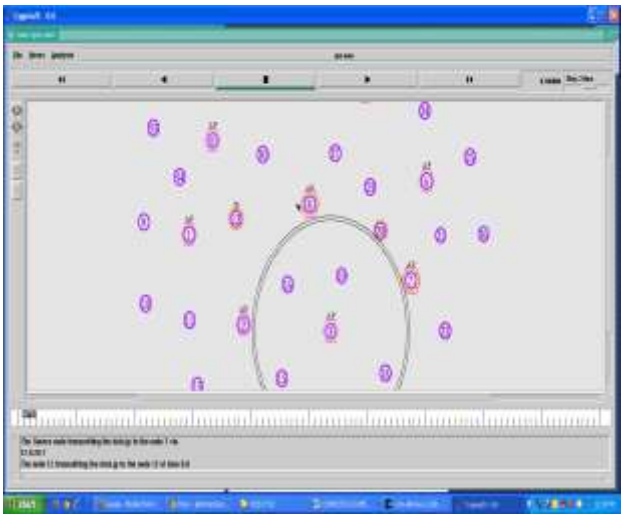


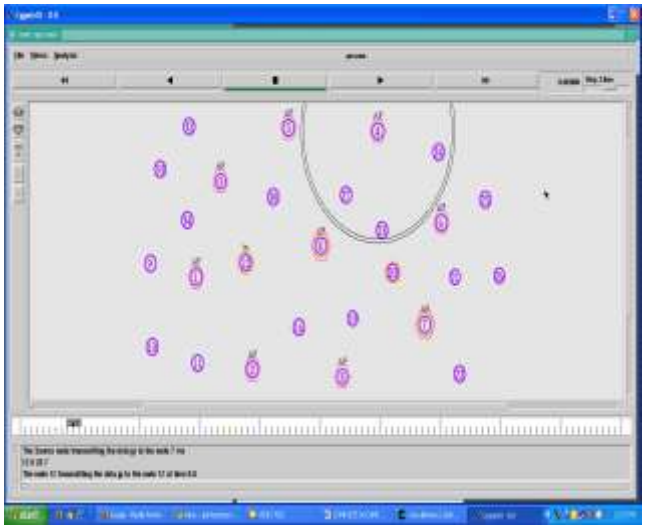
Fig 4.6: FIND ACCESS POINT

The above screen displays the node arrangement in network simulator. All nodes are arranged in random manner. To find out the access points between the source and destination. Then only we send the data in source to destination using access point.

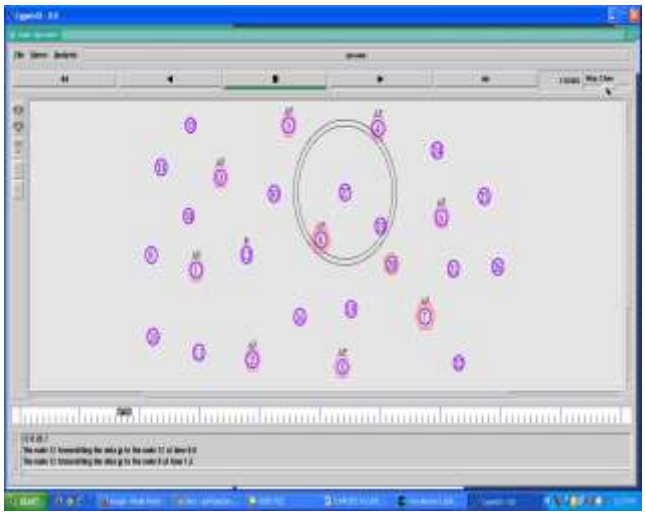
DATA TRANSMISSION PATH



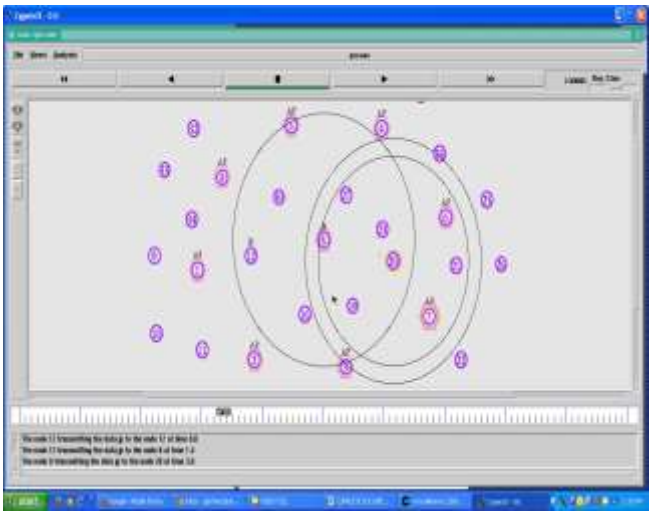
STAGE 1



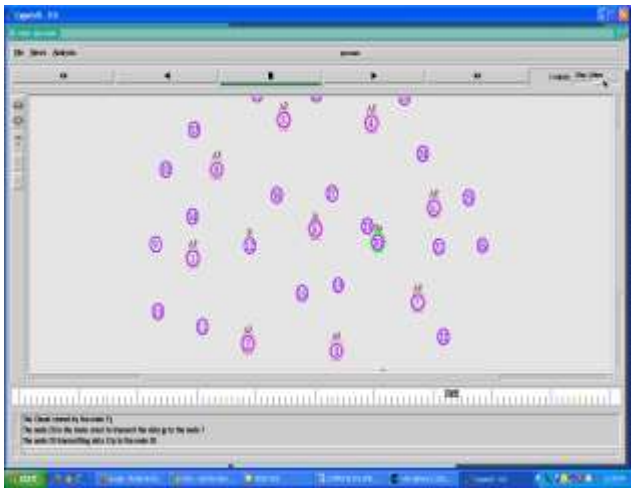
STAGE 2



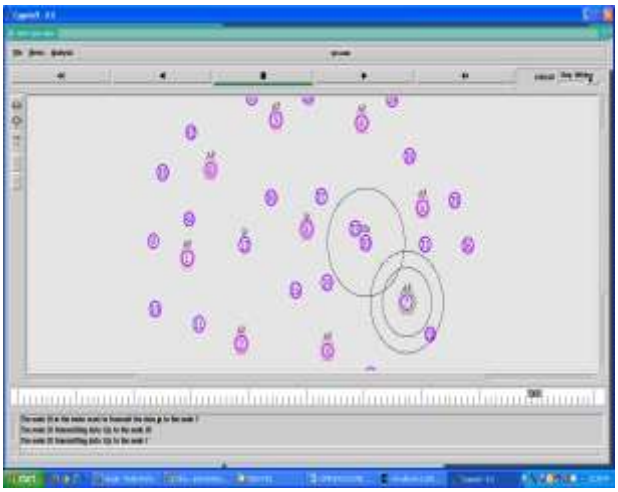
STAGE 3



STAGE 4



STAGE 5



STAGES 6

The above screen indicate the data transferring from one access point to another access point.

4. V. CONCLUSION

We have proposed an efficient network coding based privacy-preserving scheme against traffic analysis and flow tracing in multi-hop wireless networks. With the lightweight homomorphic encryption on Global Encoding Vectors (GEVs), the proposed scheme offers two significant privacy preserving features, packet flow untraceability and message content confidentiality, which can efficiently thwart Traffic analysis / flow tracing attacks. Moreover, with homomorphic encryption, the proposed scheme keeps the essence of random linear network coding, and each sink can recover the source messages by inverting the GEVs with a very high probability. The quantitative analysis and simulative evaluation on privacy enhancement and computational overhead demonstrate the effectiveness and efficiency of the proposed scheme.

5. VI. REFERENCES

[1] A. Broch, Marwan Krunz," Detection of Malicious Packet Dropping in Wireless Ad HocNetworks Based on Privacy-Preserving Public Auditing" in Proc. IEEE Int. Conf. Netw. Protocols vol. 8, no. 5, pp. 579–592, Oct. 2003

[2] A. Johnson, D. A. Maltz, , "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," in Ad Hoc Networking. Reading, MA, USA: Addison-Wesley, 2001,ch. 5, pp. 139–172.

[3] B. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," presented at the First Workshop Modeling Optimization Mobile, AdHoc Wireless Netw., Sophia Antipolis, France, 2003.

[4] C.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.

[5] C.Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM Conf., Mar. 2010, pp. 1–9.

[7] D. 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.

[8] D. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007,pp. 598–610.

[9] D. Xue and K. Nahrstedt, "Providing fault-tolerant ad-hoc routing service in adversarial environments," Wireless Pers. Commun., Special Issue Secur. Next Generation Commun., vol. 29, no. 3, pp. 367–388, 2004.

[10] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Routing amid colluding attackers," in Proc. IEEE Int. Conf. Netw. Protocols, 2007,pp. 184–193.

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

[12] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation- based incentive scheme for ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 825–830.

[13] W. Buttyan and J. P. Hubaux, "Stimulating cooperation in self organizing mobile ad hoc networks," ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.

[14] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. ACM MobiHoc Conf., 2005, pp. 46–57.

