Anonymous Secure Reputation Routing System For Selective Forwarding Attacks In Wireless Sensor Networks

[1]Dr.V.Thirunavukkarasu, [2]Dr.A.Senthil kumar, [3]K.T.JayaBharathi

[1]Professor, Government College of Engineering, Bodinayakkanur.

[2]Associate Professor, Kings Engineering College, Chennai.

[3]PG scholar, TPGIT, Vellore.

Abstract

Wireless Sensor Networks (WSNs) are more vulnerable to various security threats. One of the most important threat is selective forwarding attacks which maliciously drop a subset of packets which are being forwarded hence it makes the resource unavailable to its intended users. Due to this drop the packet loss rate is high and hence it poses a great challenge to differentiate between the normal loss and the malicious drop. In this paper, an anonymous secure routing and reputation system which detects the compromised nodes are combined where the malicious drop can be identified and reduced. Simulation results demonstrate that anonymous secure reputation routing system is more efficient than the reputation system. Further this type of authenticated secure routing improves the data delivery ratio of the network.

***Keywords**: Wireless Sensor Network, selective forwarding attack, packet dropping, Anonymous authenticated routing, onion routing.*

1. Introduction

Wireless Sensor Networks have gained much more importance over wired networks due to their costs and because of their reliability. Wireless sensor network has been widely used in homeland security monitoring and health care monitoring. But due to the drop of packets by the compromised nodes which exhibits a anamolous behavior called malicious behavior the packet loss rate during the communication of sensor nodes are very high. A reputation system uses a optimal threshold value to detect the malicious drop by the compromised nodes. However the nodes inside the network are also not trusted since it may be attacked by the physical adversaries and hence becomes malicious. As a result, anonymous authenticated secure routing is very important in adversarial environments in order to reduce the malicious drop.

When a mobile node fails to provide Integrity, Confidentiality, Availability, Authenticity, Non-Repudiation or reliability then it is called as malicious behavior [1]. Pseudonymity allows users to run services or access resources without having to reveal their own identity. This type of anonymous communication can be described as a combination of unlinkability and unidentifiability. The key for introducing the secure implementation of the anonymous communications is development of appropriate anonymous secure routing protocols [2].Since the normal packet loss has been hidden from the malicious drop, a reputation system has been used in order to monitor the forwarding behavior of the sensor nodes and to detect the malicious drop [3]. The nodes which are found as malicious are discovered and hence they are isolated to improve the data delivery ratio.

Many numbers of routing protocols have been used for anonymous secure routing. Here we consider the topology based on demand anonymous routing protocols such as AODV and DSR. Other routing protocols such as ANODR, SDAR, AnonDSR, MASK and Discount ANODR in which the unlinkability and unidentifiability are not fully satisfied. On comparing these protocols AASR is more authenticated compared to other protocols [4]-[9]. A comparative analysis on various anonymous systems have been carried out. Mix, Crowd, Hordes, Tarzan provide unlinkability but the privacy is not assured. Hence an effective routing technique called as onion routing is one of the low latency anonymous communication protocol which is resistant to traffic analysis and provides unlinkability between the responder and the messages passed. In onion routing where onion routers have messages which travel from source to destination through an unpredictable path allowing communication to be anonymous. Here every node will have information only about its previous hop and next hop.

In this paper we concentrate on notoriety framework which adaptively changes the limit esteem at whatever point activity happens in the system and furthermore used to distinguish the traded off hubs and enhance the information conveyance proportion. Despite the fact that this method segregates the sensor hubs, an assault tolerant information sending plan has been proposed to diminish the information misfortune in the system. Advance an unknown verified secure steering idea has been proposed where the system gives unlinkability and inaccessibility with a specific end goal to recognize the malevolent conduct of the sensor hubs and shield these hubs from physical foes. Broad recreation results are utilized to look at the execution of the notoriety framework and the unknown steering procedure which enhances the information conveyance proportion of the system. On looking at the outcomes, the notoriety framework recognizes the traded off hubs and confines them while utilizing mysterious secure notoriety directing framework has the course security which identifies the noxious hubs as well as enhances the information conveyance proportion of the system.

The rest of this paper is sorted out as takes after. Territory II reviews the related works. Zone III introduces the structure model and framework targets. The proposed notoriety plan is point by point in Section IV and the mysterious secure directing is resolved in Section V. Segment VI exhibits the examination of the plans for assault location. Area VII val-idates the execution of the proposed plot by broad reenactment comes about. At long last, Section VIII finishes up the paper and diagrams our future works.

2. Related Work

Most of related work focus on acknowledgment based defense technique and neighbor surveillance based defense technique in which different monitoring schemes have been adopted which monitors the data forwarding. In the following literature review, various acknowledgment schemes used for forwarding behavior and also various low latency anonymous secure routing has been discussed.

2.1. Defense Techniques

In affirmation based guard system, the hubs utilize affirmations to decide the parcel loss of each jump and identify the aggressors. Xiao et al. [10] propose a plan that haphazardly picks various middle of the road hubs along a sending way as checkpoints to return affirmations for each got parcel. In the event that suspicious conduct is distinguished, it creates an alert parcel and conveys it to the source hub. Shakshuki et al. [11] outline and actualize an interruption identification framework, named Enhanced Adaptive Acknowledgment (EAACK), for portable impromptu systems.

Also, EAACK embraces a computerized signature with affirmation to guarantee confirmation, honesty, and non-renouncement. As a versatile assessment conspire, notoriety framework is additionally connected to assault identification. Zhang et al. [12] build up a review based bad conduct location framework to coordinate notoriety administration, reliable course revelation, and distinguishing proof of getting into mischief hubs in view of conduct reviews in impromptu systems. With the Watchdog hardware [13], sensor nodes can monitor the forwarding behaviors of their neighboring nodes and record the actual packet loss accurately. In [14], SCM use the nodes adjacent to a data communication route, to constitute a side channel for monitoring the forwarding behaviors of the nodes en route. Hence the malicious nodes can be identified.

2.2. Anonymous low latency network systems

Anonymous communication systems over the internet can be classified into two categories as systems for high latency applications and system for low latency applications [15]. In the mix type anonymous routing where the sender is not known while the receiver is known hence it provides unlinkability but has timing attack. In crowd, there is no privacy and hence the sender is not known while the receiver is known while suffers from denial of service attack. Tarzan is another low latency anonymous system based on peer to peer architecture which provides minimal protection against timing attack. In the onion routing technique, the sender and the receiver are anonymous and hence provide high unlinkability and unavailability of the resources to the attackers [2].

2.3. Anonymous on demand routing protocols

Anonymous on demand routing protocols are classified into two categories as topology based and location based. The various protocol comparisons have been discussed. ANODR and ASR uses anonymous virtual circuit routing and data forwarding. SDAR and AnonDSR are anonymous routing protocols with the combination of proactive MIX net. MASK relies on proactive neighbor detection protocol to constantly see snapshot of the one hop mobile neighborhood [16]. RAODR deploys a master key mechanism but cannot provide anonymity, traceability and enforceability that are supported by a group signature. Compared to above protocols AASR provides higher throughput and lower packet loss ratio in different mobile scenarios in presence of adversarial attacks and also provide secure communication [2].

Compared to previous work on malicious node detection through threshold value where malicious nodes are isolated, in this paper we determine the adaptive detection threshold value which changes based on the traffic in the network flows and hence detects the malicious nodes and isolates them. But in anonymous secure routing AASR can detect the malicious node via the group signature and hence malicious nodes are detected via the routing table. On combining the anonymous routing with the reputation system routing is secure compared to the reputation system on detection of malicious drop. Comparisons on these techniques have been outperformed which improves the data delivery ratio of the network and throughput of the network with reduced delay in the network.

3. System Model and Design Goals

3.1. Network Model and Attack Model

Remote sensor systems (WSNs) are defenseless against various sorts of security dangers that can corrupt the execution of the entire system and that may bring about lethal issues like Denial Of Service (DoS) assaults, directing assaults, Sybil assault and so forth. Key administration conventions, confirmation conventions and secure steering can't give security to WSNs to these sorts of assaults. Interruption Detection System (IDS) is an answer for this issue. It investigates the system by gathering adequate measure of information and identifies irregular conduct of sensor hubs.

IDS based security components proposed for other system standards, for example, specially appointed systems, can't specifically be utilized as a part of WSNs [17]. Notoriety based frameworks utilize neighboring checking procedures to assess the conduct of hubs. A plan which depends on two modules, the guard dog and the way rater was proposed. The guard dog module is in charge of catching the transmission of a successor hub, along these lines checking the fruitful bundle sending to the following bounce. The way rater module utilizes the allegations produced by the guard dog module to choose ways free of getting into mischief hubs [12].

3.2. Adversaries and Infrastructure

Adversary knows all the protocols and the network functions and hence the passive attack is a network attack in which the system is monitored and sometimes scanned for open ports and vulnerabilities. It includes active reconnaissance and passive reconnaissance in which an intruder engages with the targeted system to gather information about vulnerabilities it is said to be active and when it attempt to gain information about targeted computers and networks without actively engaging with the systems is said to be passive. Passive attacks are often preparatory activities for active attacks. Public Key Infrastructure (PKI) includes the key elements such as Certificate Authority(CA) [2].

3.3. Node Model

A node is either a redistribution point or a communication end point. A physical network node is an active electronic device that is attached to a network and is capable of creating, receiving, or transmitting information over a communication channel. The source node knows all its possible destination nodes and the destination information is stored in the destination table. Every node changes its information locally and hence it generates different pseudonyms to communicate with its neighbors. Source send route request to neighbor node including its pseudonym, public key, and destination string. The destination string destination is a binary string, which means "You are the destination" and can be recognized by D. If there is no session key, S will generate a new session key KSD for the association between S and D. Then intermediate node decrypt the message if its success then reply message to source otherwise it again broadcast message to its neighbor until reach destination. The forwarding table or forwarding information base or MAC table, used in bridging the network, routing and similar functions with proper interface to which the input interface should forward a packet.

3.4. Design Goals

The objective of this paper is to detect the selective forwarding attack by means of reputation system and also with the help of authenticated secure routing technique. These two methods are very useful in isolating the malicious nodes and also to create an authenticated secure routing technique where they are anonymous to their neighborhood sensor nodes. With these two techniques it has high detection accuracy and also has a high data delivery ratio. The authenticated anonymous secure reputation routing system is more effective.

4. Reputation System

In this section we propose a reputation system which is used to detect the selective forwarding attacks in wireless sensor networks. This reputation system selectively drops the packets hence we are unable to identify whether it is a normal packet loss or malicious drop. Normal packet loss caused by radio link quality and MAC layer collisions. Radio link quality is the primary reason due to poor and unstable radio link quality for the time varied conditions. The packet loss rate is determined as an average value over a long term period.

However adopting an average value to represent a time varied value which may mislead the evaluation of forwarding behaviors. The link quality is estimated by means of Received Signal Strength Indicator (RSSI) and Signal to Noise Ratio(SNR) under the symmetric channel condition. As data transmission between two neighboring nodes is based on IEEE 802.11 DCF, MAC layer collisions may increase the normal packet loss rate of the network [3].

In this technique a reputation system has been used where the reputation scores are stored in the reputation table. The reputation system evaluates the reputation values of the neighboring nodes and hence the reputation scores are propagated and hence integrated and updated in the reputation table. Hence from the reputation scores malicious nodes are identified based on the optimal threshold value and hence the threshold value changes based on the traffic condition. The nodes which are been found as malicious are isolated. The malicious nodes are evaluated based on the forwarding behavior of the sensor nodes and hence been updated in the reputation table.

An attack tolerant routing scheme has been proposed for data forwarding which improves the data delivery ratio of the network. Dynamic routing technique improves the detection accuracy with high delivery ratio of the network. To choose a superior sending hub to improve the information conveyance proportion, we present the normal data forwarding ratio (DFR), which is characterized as the proportion between the normal number of sent information parcels and the all out number of sent information bundles. In every assessment period the source hub choses the hub with the most elevated DFR from its sending applicant set as the following jump.

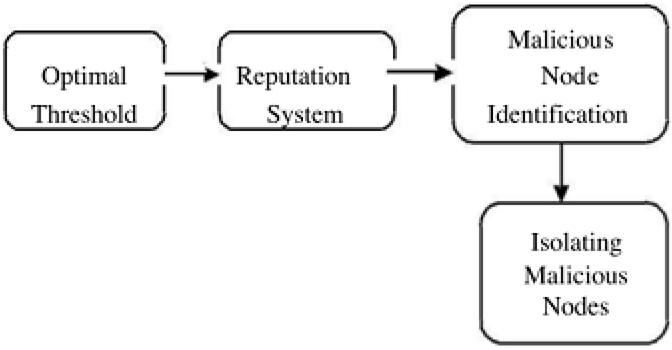


Fig. 1. Architecture of reputation system

Meanwhile due to malicious node detection the cooperation simulation and overhead can be reduced by means of a PROBE packet [3]. Nodes with low attack probability avoid reputation punishment and the nodes with high attack probability can be remove by the security check soon.

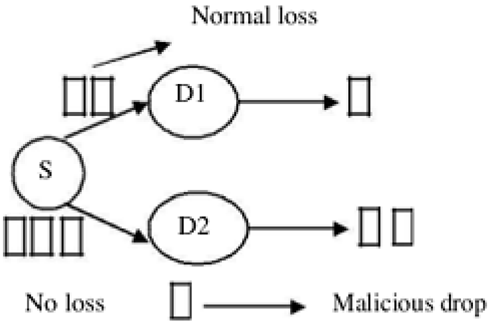


Fig. 2. Routing technique

5. Anonymous Routing

In this section, AASR protocol have been used. Here a anonymous authenticated routing technique known as onion routing has been used. In onion routing technique the onion routers messages travel from source to destination. Here the sender and the receiver are anonymous so that security is authenticated while data transmission.

Let us consider the source be S and the destination be D while X, Y, Z be the intermediate nodes. Now the source S discovers the route for destination D. Here the source sends the RREQ to the neighboring nodes where the message is being encrypted. Once Y receives the RREQ packet it will verify the packet with its group key. Encryption is done by the public and private key. Decryption is done by layer and layer and hence on receiving RREP message the packets will be transmitted. Since there will be anonymous data transmission the malicious nodes can be detected and hence the route pseudonym can be recognized by the downstream nodes.

ISSN: 2005-4238 IJAST

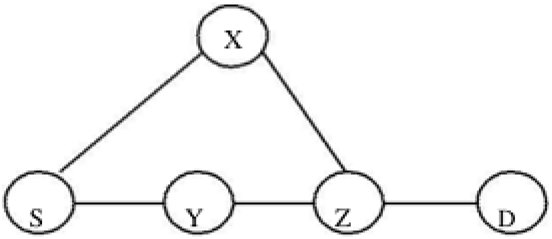


Fig. 3. Topology of the network

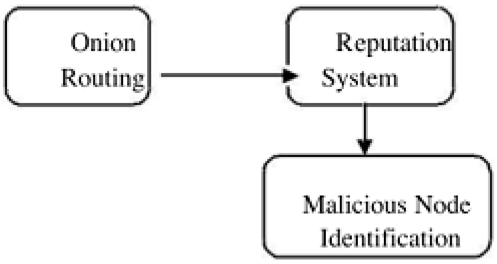


Fig. 4. Anonymous secure reputation routing system

In the above figure the onion routing technique has been proposed which secures the route from malicious drop and it is combined with the reputation system so that the malicious drop is reduced and hence isolation of malicious nodes are much reduced.

The directing calculation can be actualized in view of the current on-request impromptu steering convention, for example, AODV or DSR. The principle steering strategies can be abridged as takes after.

1. During course revelation, a source hub communicates a RREQ bundle.
2. If a middle of the road hub gets the RREQ parcel, it confirms the RREQ by utilizing its gathering open key and includes one layer top of the key-encoded onion. This procedure is rehashed until the RREQ bundle achieves the goal or lapses.
3. Once the RREQ is gotten and checked by the goal hub, the goal hub collects a RREP bundle and communicates it back to the source hub.
4. On the switch way back to the source, each moderate hub approves the RREP bundle and updates its steering and sending tables. At that point, it evacuates one layer on the highest point of the key-encoded onion and keeps broadcasting the refreshed RREP.
5. When the source hub gets the RREP parcel, it confirms the bundle and updates its directing and sending tables. The course revelation stage is finished.
6. The source hub begins information transmissions in the set up course. Each middle of the road hub advances the information bundles by utilizing the course alias.

Here with the blend of onion directing and the notoriety framework the steering is extremely secure and henceforth noxious drop can be effortlessly evaded if subsequently this drop happens then by the use of notoriety framework pernicious drop can be effectively identified and disengaged.

6. Performance Evaluation

The compromising probability in this network scenario is less than 80%. Hence the compromising nodes which are less than 80% considered as compromised malicious nodes and hence they are isolated. The security check is evaluated in each evaluation period and hence it improves the attack detection accuracy and the data delivery ratio also improves. In anonymous secure reputation routing system, the malicious nodes can be detected via the group signature and get rid of the attackers by means of routing table. On comparing these techniques, the packet received ratio and throughput are high in reputation evaluation when compared to anonymous secure reputation routing system.

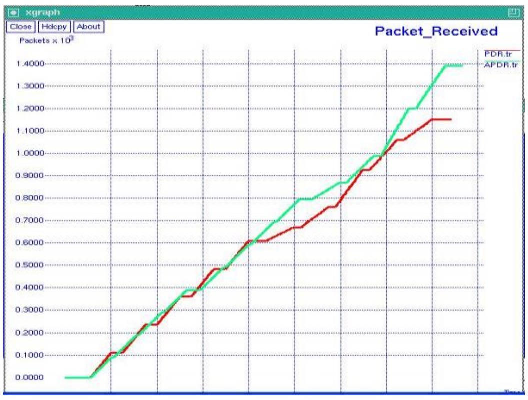
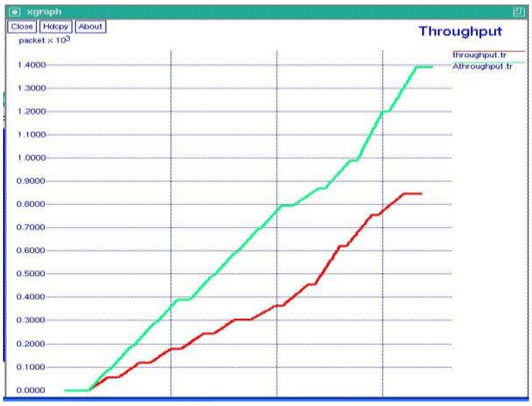


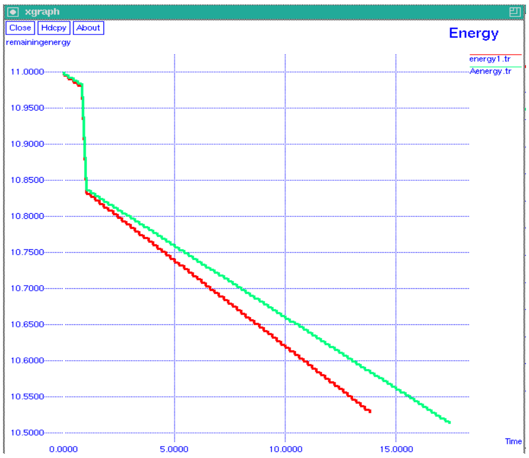
Figure. 5. Performance Comparisons

6.1. Packet Received Ratio

With this technique the sender is anonymous so that the routing is so secured and hence by using the reputation system the malicious nodes are identified and isolated. Since the identity, route and location are anonymous. Passive attacks, impersonation attack and denial of service attacks are reduced with the help of group signature.



6.2. Per flow throughput

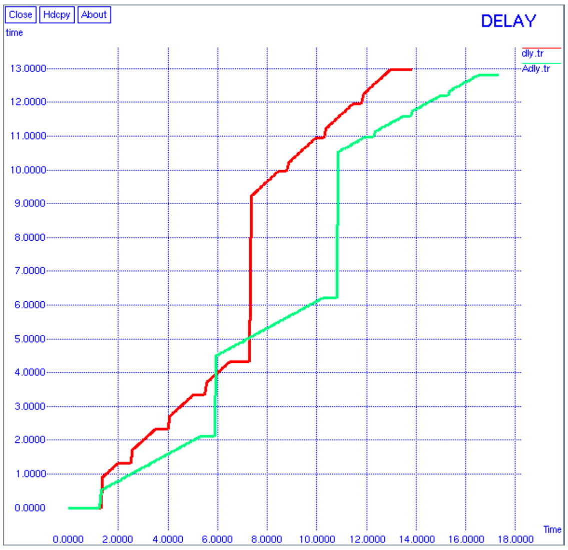


ISSN: 2005-4238 IJAST

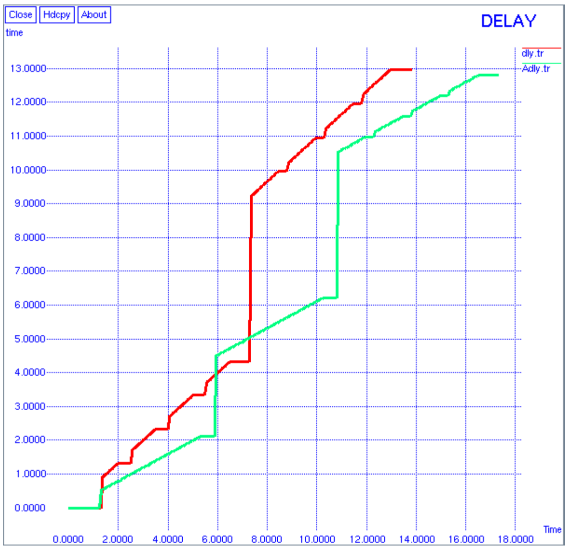
6.3. Energy flow

With the reputation system the malicious nodes are identified and then isolated. Hence this type of routing system uses the onion routing technique with the reputation system which helps us to improve the packet received ratio and also throughput of the network with the reduced delay with the improved energy based on the optimal value the packet dropping nodes can be easily identified with this anonymous secure reputation routing system which supports high data security.

Here by combining anonymous secure routing with the reputation system the packet received ratio and the throughput are improved.



6.4. End to end delay



7. Conclusion

In this paper, we have designed a reputation system and an authenticated routing technique in order to detect the malicious nodes. Here in reputation system the malicious nodes are isolated but in onion routing the message has been encrypted and decrypted in onion by means of group signature and hence the malicious nodes are detected and hence the message is authenticated. Reputation system uses the threshold value which is combined with anonymous routing so that malicious node can be easily identified and isolated. Here anonymous secure reputation routing system provides higher throughput and high packet delivery ratio with reduced delay. In our future work, we will focus on improving ASRRS hence concentrate on the reputation system in mobility of sensor nodes and also delay and packet loss ratio in the mobile nodes.

References

[1] Akshay Narayan Hedge, Vinay Kumar, Prof. Vijayan, "Self Routing: A novel based approach for context based trust evaluatin and malicious node detection in MANET," International journal of pharmacy and technology, August2016.

[2] Wei Liu and Ming Yu, "Authenticated Anonymous Secure Routing for MANET's in Adversial Environments," IEEETransactions on Vehicular Technology, vol 63, No.9, Nov.2014.

[3] Ju Ren, Yaoxue Zhang, Kuan Zhang and Zuenium Shen, "Adaptive and Channel aware Detection of selective forwarding attacks in wireless sensor networks," IEEE Transactions onWireless Comm. Vol. 15 No. 5, May 2016.

[4] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, Jul. 2003. [Online]. Available:www.ietf.org/rfc/rfc3561.txt

[5] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for MobileAdHocNetworks for IPv4,"IETFRFC4728, Feb. 2007.[Online]. Available: www.ietf.org/rfc/rfc4728.txt

[6] J. Kong and X. Hong, "ANODR: ANonymous on demand routing with untraceable routes for mobile ad hoc networks," in Proc. ACM MobiHoc, Jun. 2003, pp. 291–302..

[7] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A secure anonymous routing protocol for wireless and mobile ad hoc networks," in Proc. IEEE Int. Conf. LCN, Nov. 2004, pp. 618–624.

[8] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient anonymous dynamic source routing for mobile ad hoc networks," in Proc. ACM Workshop SASN, Nov. 2005, pp. 33–42.

[9] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in Proc. IEEE INFOCOM, Mar. 2005, vol. 3,pp. 1940–1951.

[10] B. Xiao, B. Yu, and C. Gao, "CHEMAS: Identify suspect nodes selective forwarding attacks," J. Parallel Distrib.Comput., vol. 67, no. 11, 2007

[11] E. Shakshuki, N. Kang, and T. Sheltami, "EAACK—A secure intrusion-detection system for MANETs," IEEE Trans. Ind.Electron., vol. 60, no. 3, pp. 1089–1098, Mar. 2013.

[12] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," IEEETrans. Mobile Comput., Sep. 2013.

[13] T. Shu and M. Krunz, "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing," in Proc. 5th ACM Conf. Security Privacy WirelessMobile Netw. (WiSec), 2012, 87–98

[14] X. Li, R. Lu, X. Liang, and X. Shen, "Side channel monitoring: Packet drop attack detection in wireless ad hoc networks," in Proc. IEEE Int. Conf. Commun. (ICC), 2011, pp. 1–5.

[15] Rungrat Wiangsripanawan,willy susilo and Rei Safair Naini, "Design principles for low latency Anonymous network systems secure against timing attacks," Center of information security ,March 2014.

[16] Ju Liu, Jiejun Kong, Xiaoyan Hong, Mario Gerla, "Performance Evaluation of Anonymous Routing protocols in MANETs, April 2015.