An Improved Trust Aware Routing Protocol for Wireless Sensor Networks

[1] Ballina Mohana Lakshmi,
[1] M.tech scholar, Department of Computer Science and Systems Engineering,
Andhra University, Visakhapatnam, Andhra Pradesh, India

[2] D. Lalitha Bhaskari,
[2] Professsor, Department of Computer Science and Systems Engineering,
Andhra University, Visakhapatnam, Andhra Pradesh, India.

Abstract: Wireless Sensor Networks is an emerging and challenging technology with low processing and battery power. Security becomes a major issue in wireless sensor networks because of its wireless nature; it is prone to various types of attacks and loss of data packet. In this paper, various security mechanisms are discussed to find malicious nodes and to do secure routing. In the proposed work, our main aim is to find the trusted node by using a trust model and the malicious report is checked, and routing is done. It provides security features with minimum overhead and energy efficiency. Trust-aware routing protocol plays a vital role in the security of wireless sensor networks, which is one of the most popular network technologies for the smart city. However, several key issues in conventional trust-aware routing protocols remain to be solved, such as the compatibility of trust metric with quality of service metrics and the control of overhead produced by trust evaluation procedure. This paper analyzes the features of common attacks on trust-aware routing schemes, then, specific trust computation and trust derivation schemes are proposed based on analysis results. Finally, our design uses the combination of trust metric and quality of service metrics as routing metrics to present an optimized routing algorithm. From the simulation, centralized secure routing can achieve both intended security and high efficiency.

***Index Terms* – Wireless Sensor Networks, Secure routing, Security, Energy efficient, Communication trust, Data trust, Optimal route, Trust management.**

I. INTRODUCTION

Since years, the monitoring of areas of interest is a topic of great importance for civil as well as military applications, such as emergency scenarios, manufacturing environments, battlefields, etc. Due to the advances in microelectronics, highly integrated electronics, and improved energy accumulators, in the last few years, the development of sensor nodes was intensified so that the sensor nodes got smaller and smaller, while the price per sensor went down at the same time. One of the major ideas was that the sensor nodes should form a collaborative wireless network to monitor events in arbitrary environments by acting in a self-configurable, self-organizing adhoc manner, i.e. without the necessity of human interaction. Wireless sensor networks (WSNs) are emerging technologies that have been widely used in many applications such as emergency response, healthcare monitoring, battlefield surveillance, habitat monitoring, traffic management, smart power grid, etc. However, the wireless and resource-constraint nature of a sensor network makes it an ideal medium for malicious attackers to intrude the system. Thus, providing security is extremely important for the safe application of WSNs. WSNs are a collection of nodes where each node has its own sensor, processor, transmitter, and receiver.[1] The sensors are low-cost devices that perform a specific type of sensing event. Being of low-cost such sensors are deployed densely throughout the area to monitor the specific event. WSN are highly distributed networks of small lightweight wireless nodes. Sensor nodes are called as a mote.[3,4] It monitors the environment or system by measuring physical parameters such as temperature, pressure, humidity, etc. Sensor networks are widely applied in various filed such as environment monitoring, military applications, health care, and home intelligence. Since, the sensor's energy, in most cases a battery that should last for the sensor's lifetime, is strongly limited, the sensor nodes are constrained in their computational power, memory and transmission range. As a consequence, the nodes can neither perform computationally intensive tasks nor deliver meaningful results by acting on their own. Therefore, the sensor nodes have to cooperate to be able to monitor bigger areas, aggregate measured values and transfer them to a point in the network where the data can be read out and evaluated. One of the major research areas in WSNs is the routing of data packets from a source to a destination through the network. Because of the limited energy resources, energy is one of the primary design requirements for routing protocols in WSNs. To save energy the transmission range of each sensor is severely limited so that data packets that should be transmitted across the network have to be forwarded [2] via multiple hops. Due to topology changes, interferences caused by environmental influences or adversaries, node failures or perishing energy resources, the routing has to be failure-tolerant and has to adapt permanently, while using as little energy as possible. With up-to-date routing, information packets can be routed around critical areas so that a complete breakdown of the network can be avoided. Furthermore, the routing algorithm should take load balancing into account to avoid overloading of certain nodes to reduce the risk of partitioning the network,[5]Leading to missing paths between the source and the destination. Moreover, the fusion of sensed data needs to be considered in WSN routing protocols to reduce redundant transmissions of the same data. Wireless sensor networks are a wireless network consisting of spatially distributed autonomous devices using sensors to monitor the physical and environmental condition. Critical vulnerabilities such as node capture and denial-of-service (DoS) attacks. Various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to reduce security threats such as eavesdropping, message reply, and fabrications of messages. Sensor nodes are small in size and able to sense events, process data, and communicate with each other to transfer information to the interested users. Typically, a sensor node consists of four sub-systems:-

- Computing subsystem (processor and memory).
- Communication subsystem (transceiver).
- Sensing subsystem (sensor).
- Power supply subsystem (battery).

WSNs are a collection of self-organized sensor nodes that form a temporary network. In a wireless sensor network, the trust specifies the reliability or trustworthiness of a sensor node. In this, the trust model specifies & plays an important role in identifying misbehavior nodes and providing collaboration among trustworthy nodes. The reputation-based framework for high integrity sensor network was first trust-based model designed and developed for sensor networks. Trust is defined as a belief level that one sensor node puts on another node for a specific action according to the previous observation of behaviors. Trust value ranges from 0 to 1 where 1 is completely trustworthy. Trust is of mainly three types, they are as:-

- Direct Trust: based on direct communication behaviors.
- Recommendation Trust: filtered recommendations for 1-hop nodes.
- Indirect trust: trust for multi-hop nodes based on recommendations.

II. BACKGROUND TECHNOLOGY

This section deals with background techniques such as WSN, secure routing, challenges, Agent technology.

A. Wireless Sensor Networks (WSN)

WSN consists of sensors that are randomly distributed in an ad hoc manner. The sensor nodes sense some physical phenomenon and then the gathered information is processed. Although deployed in an ad hoc manner it needed to be self-organized and self-healing.WSN provides a bridge between the physical and virtual worlds. The Sensor has limited sensing regions, processing power and energy. Each node of the sensor network consists of four subsystems: the sensor subsystem senses the environment, the processing subsystem performs computations on the sensed data, and the communication subsystem is responsible for message exchange with neighbor sensor nodes and power unit. A Sensor network is designed based on low node cost, low power consumption, self-configurable, scalability, adaptability, reliability, fault-tolerant, QOS, support, and security.

Energy efficiency is more important in a sensor network to ensure network performance and prolong the network lifetime. The main reason for waste of energy are ideal listening, collision, overhearing, control overhead, in medium access unlike MAC protocols, WSN schemes must allow sleep modes during radio inactivity to maximize energy efficiency. Two main classes of protocols are contention-based and contention-free. Routing in wireless sensor networks can be made robust and efficiency by incorporating different types of local information such as link quality, link distance, residual energy, and position information. Overhead includes the processing time, storage, memory consumption for a process.

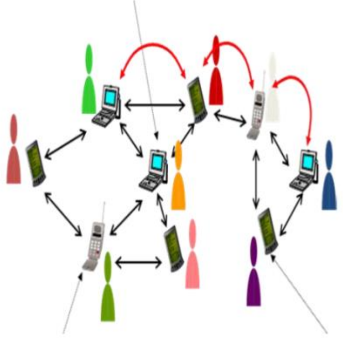


Fig.1 Various nodes connected in WSN

B. Security Issues in WSN

Wireless sensor networks are vulnerable to security attacks due to the broadcast nature of the wireless transmission medium. The attacks are broadly classified into two categories as active and passive attacks [2]. The monitoring and listening of communication channels by unauthorized attackers are known as passive attacks. Some of the attacks are monitor and eavesdropping, traffic analysis. The unauthorized attacker's monitors, listen and modify the data in a channel are known as active attacks. The active attacks are attacks on the information in transit, selective forwarding, black hole, and sinkhole, hello flood attacks and denial of services. These attacks are the significance of malicious nodes in wireless networks.

Monitor and eavesdropping:- Eavesdropping is secretly listening to the private conversation. The eavesdropping attack is a serious security threat to WSN. In this malicious node detect the information by listening to the message transmission in the wireless medium. And also malicious node steals the information by sending queries to transmitters by disguising themselves as friendly nodes. This attack is also known as a confidentiality attack.

Selective forwarding: - A malicious node can selectively drop only some packets. This dropping of node increases when it is combined with sinkhole or acknowledgment spoofing. The attack can be used to make a denial of service attack targeted to a particular node. In this, the malicious node will behave like a black hole and refuses to forward the packet [5].

C. Challenges

The Wireless medium is less secure because it's broadcast nature makes eavesdropping simple. The Wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Adhoc nature of sensor networks means no structure can be statically defined. Nodes may fail or be replace the network that must support self-configuration. Sensor nodes are deployed in a hostile environment; it faces the possibility of destruction or capture by the attackers. Providing security in WSN is even more difficult in MANETS due to the resource limitation of sensor nodes and security concerns remain a serious impediment to the widespread adaptation of these WSNs [4]. The highly hostile environment represents serious challenges for security researches. The Secure model should use battery life efficiently. WSN goals [3] include confidentiality, Integrity, Data origin authentication, Access control, Availability. It has to design against the attack such as eavesdropping, fabrication, injection, modification, node capturing.

D. Secure Routing

Routing is one thing that distinguishes WSN from MANET and other networks. Routing is a challenging task in WSN because the number of sensor nodes is deployed in the ad monitoring area. Because of wireless nature the WSN prone to various types of security issues, routing is one main area that has to focus. Secure routing has to be done to avoid signal spoofing, injection of a fabricated message into the network, alteration of messages while transmission, avoid the formation of loops, avoid redirection of shortest path [19]. System fault, error data may also cause network failure. To overcome the attacks and information loss, secure routing has to be done [20]. Secure routing through the trusted node is one of the ways to avoid the attacks mentioned above. Secure routing protocol has to consider the sensor network limitation such as limited memory, energy, resource-constrained.

E. Trusted Node

Trust has to establish between nodes to ensure the trustworthiness of the node. A Trusted node refers to the node which behaves normally, that is sensing and forwarding packets to the proper destination without any information loss. Many types of schemes are used to find the trusted node and detection of a malicious node, some of them are discussed here. In Trust based method, Trust values can be calculated from the reputation and behavior of the node [20]. The system is given with the threshold above the threshold the node is normal otherwise it is malicious. In cryptography key exchange mechanisms used to find malicious nodes.

F. Agent Technology

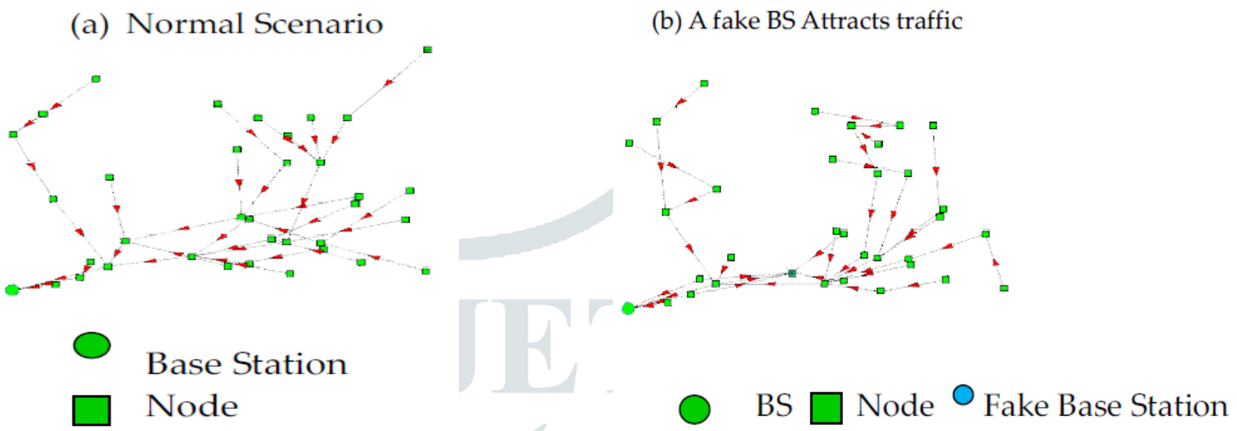
A Software agent is a persistent, goal-oriented computer program that reacts to its environment and runs without continuous direct supervision to perform some function for an end-user or another program. The agents offer effectiveness, efficiency, transparency, and optimization. The agents are mobile and static. Mobile agents move from system to another and do their execution, features include autonomy, learning. Static agents are static, it does the same work as mobile agents other than mobility.

III. LITERATURE SURVEY

In this paper [17] they propose a trust and energy-aware, it is a location-based protocol for WSN. The trust values are calculated and in addition to that we are adding location and energy to find the trustworthy path [18]. This method consists of two phases, the setup phase, and the forwarding phase. In the setup phase, each node calculates its cost value based on the trust values, the energy level of the neighbor node, location based on the distance between the node to the neighbor node, and the node to the base station. So the next best hop node is selected based on the trust value, energy level, and location information. If the cost value is low, that node is chosen to send the packets. In the forwarding phase, the node forwards the packet depending on its trustworthiness of packets; it is determined by the trust value of source node, trust limit, and MAC. It has Load balancing capacity and Energy-efficiency. The Setup phase is done often when the network size increases.

IV. PROPOSED WORK

In our work, the study is done based on the basic requirement as Energy efficiency, overhead, and security features include authentication, data confidentiality, and integrity. Energy efficiency is the goal and is achieved with minimum energy, overhead is due to memory, computation time.



Cryptography is the method of encrypting the message using the key, it can be decrypted only the key is known. From the survey, we identified that the system which offers energy efficiency, less overhead and security features are considered as the best scheme to route the data packet securely. Existing work did not achieve the security goals, with minimum energy and overhead and also it does not provide the option for checking whether the reported malicious node is true or not. With this concern, the new algorithm is proposed.

The proposed work is a trust model consists of a probability model, MAC model, EAACK based on Misbehavior node verification, and routing through the trusted node. The Proposed model includes
(i) Identification of trusted node
(ii) Routing through the node.

Identification of Trusted Node:

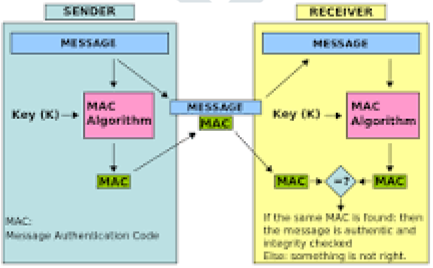

SENDER
MESSAGE
Key (K)
MAC Algorithm
MAC
MAC:
Message Authentication Code
MESSAGE
MAC
RECEIVER
MESSAGE
Key (K)
MAC Algorithm
MAC
=?
MAC
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

Fig.2 Identification of Trusted Node

In Fig.2, we can find the trusted node based on the probability model and MAC (Message Authentication Code) model. The Probability model gives trust value based on the behavior of the node. In the MAC model, the verification of MAC is done.

If the MAC does not match, it goes to secure Acknowledgement mode. The report is sent to the source and verifies the reported node by using the misbehaving report phase.

Routing through the node:

1. Once the trusted node is found the BFS algorithm is implemented.
   The working procedure is explained below

Step1:

i. Select the Probability model

ii. Assume a threshold value as 0.5,

iii. The nodes are given a rating based on the node's behavior.

iv. If rating above 0.5, considered as a trusted node

v. Otherwise, it is untrusted.

Step2:

i. Select the MAC model

ii. In this, the message is encrypted by using the key, and it is sent to the trusted nodes. The message is recomputed and MAC is checked. Mobile agents are responsible for carrying the encrypted message to check the MAC verification.

iii. If it is matches considered as a trusted node and sends Ack to the source.

iv. Otherwise, move to step3

Step3:

i. Secure Acknowledgement (ACK) phase

ii. Insecure acknowledgment (S-ACK) phase three nodes work together to find the malicious node, the node R4 sends S-ACK data packet (pkt1) to R5, then R5 forwards

- R1-R2-R3-R7-R5-R6-R12,
- R1-R8-R9-R10-R11-R12,
- R1-R8-R9-R10-R5-R6-R12.

this packet to i6.the node R6 receives the pkt1 it has to send the S-ACK packet to R4.

iii. If R4 does not receive this acknowledgment, then the node R4 is considered to be malicious. It is reported to the source

node.

iv. The source node switches to the Misbehavior Report Authentication (MRA) mode to ensure that the node is malicious

or not.

Step4:

i. Misbehavior (malicious) report phase

ii. In MRA mode, it checks whether the reported malicious node is true or not.

iii. It checks whether the missing packet is reached the destination through any other node. When the destination node receives the MRA packet, it checks its local knowledgebase.

iv. If the missed packet is already received by the destination node through a different path. It is concluded that it is a false misbehavior report. That is R4 is considered as a malicious node is not true, who generated the R6 report is considered as a malicious node.

v. Otherwise, the misbehavior report is considered as true.

The static agents and mobile agents are implanted in each node static agents trigger the mobile agent to collect the information about the trusted node and malicious node and its path towards the destination. It maintains the list of a trusted and malicious node that is identified by the proposed method. In this, we use BFS for routing. Let us consider a scenario shown in Fig.3.

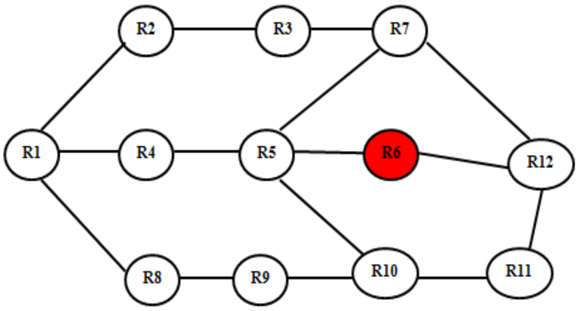


Fig.3 Network Topology

In this topology (Fig.3), R1 is a source, R12 is a destination, in this, the available path to destination are as follows

- R1-R4-R5-R6-R12,
- R1-R2-R3-R7-R12,
- R6-R12,

In this, let us consider that node R6 is malicious by the given algorithm. Suppose the route selected is R1-R4-R5-R6-R12. The mobile agent in R4 has to report the next node the path has a malicious node, so redirect the path through R7 or R8. It chooses the R7 because it is the shortest path to reach the destination. Thus the routing is done through the trusted node. The proposed work is energy efficient, offers minimum routing overhead because we use agents to provide communication.

V. SIMULATION ENVIRONMENT

The experiment was conducted using NS2 running on a personal computer (PC).

Simulation Results

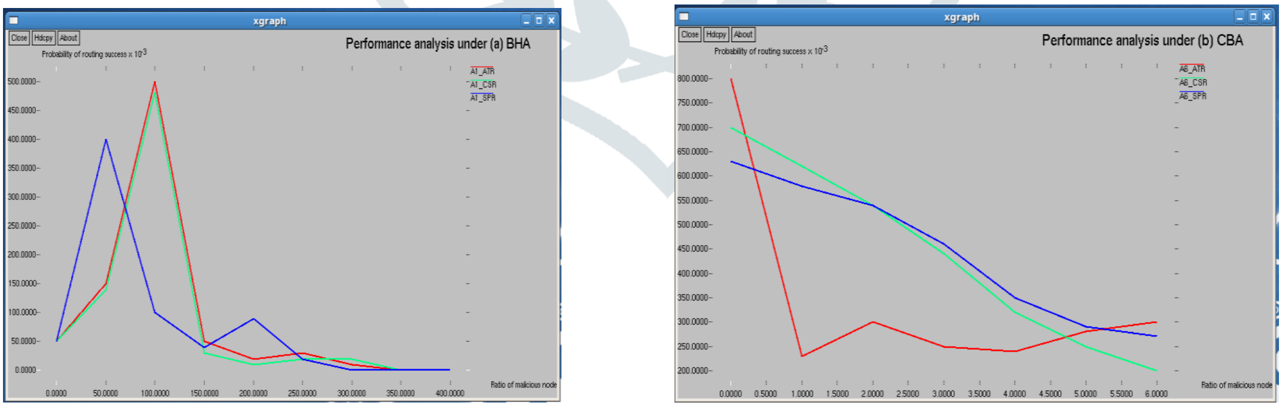


Fig.4 Performance analysis based on BHA and CBA

VI. CONCLUSION

In a wireless sensor network, the security issues are a major concern. Secure routing is one of the main concepts to achieve security in WSN. This paper discusses various existing methods to find the trusted node, secure routing and also presents a survey of the routing protocol that specifies how it provides a better routing path for transmitting the packets from source to destination dynamically. An overview of Trust aware routing protocol for secure routing in Wireless Sensor Networks and modules involved in that to improve the performance is presented. Finally, the design consists of how the modules are selecting the better route for transmitting packets. This paper presents a trusted sensing-based secure routing mechanism to handle common network attacks. An optimized routing algorithm is proposed, which considers the trust degree and other Quality of Service metrics. The Simulation results show how centralized secure routing can reduce the routing overhead and improve the reliability of data transmission compared with the traditional trust mechanism. Future research will design a distributed intrusion detection system for WSN, which may provide a new way for the research of trust degree and ubiquitous routing. Finally, it concludes that most of the work does not provide a high level of security, and secure routing with energy-efficient and reduced overhead. In the proposed work this has been taken as a major concern and designed agent-based secure routing using trustworthy nodes.

REFERENCES

[1] O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus, and A. Yener, "Transmission with energy harvesting nodes in fading wireless channels: optimal policies," IEEE Journal on Selected Areas in Communications, vol. 29, no. 8, pp. 1732-1743, Sep. 2011.

[2] N. Marlon, C. Jose, A. B. Campelo, O. Rafael, V. C. Juan, and J. S. Juan, ”Active low intrusion hybrid monitor for wireless sensor networks,” Sensors, vol. 15, no. 3, pp. 23927-23952, 2015.

[3] G. Ottman, A. Bhatt, H. Hofmann, and G. Lesieutre, ”Adaptive piezoelectric energy harvesting circuit for wireless, remote power supply,”IEEE Transactions on Power Electronics, vol. 17, no. 5, pp. 669-676, Sep. 2002.

[4] A. K. A. Mohammad, and S. Gadadhar, ”Enhancing cooperation in MANET using neighborhood compressive sensing model,” Egyptian Informatics Journal, vol. 6, no. 1, pp. 1-15, 2016.

[5] G. Uttam G, and D. Raja, ”SDRP: a secure and dynamic routing protocol for mobile ad-hoc networks," IET Networks, vol. 3, no. 2, pp. 235-243,2014.

[6] W. K. K. Chin, and K. L. AYau, "Trust and reputation scheme for clustering in cognitive radio networks," International Conference on Frontiers of Communications, Networks, and Applications (ICFCNA), Kuala Lumpur, Malaysia, Nov. 2014, pp. 1-6.

[7] Y. Gao, H. W. Chris, J. J. Duan, and J. R. Chou, ”A novel energy-aware distributed clustering algorithm for heterogeneous wireless sensor networks in the mobile environment,” Sensors, vol. 15, no. 10, pp. 31108- 31124, 2015.

[8] J. G. Choi, S. Bahk, ”Cell-throughput analysis of the proportional fair scheduler in the single-cell environment,” IEEE Transactions on Vehicular Technology, vol. 56, no. 2, pp. 766-778, 2007.

[9] K. B. Sourav, and M. K. Pabitra, ”SIR: a secure and intelligent routing protocol for vehicular ad hoc network,” IET Networks, vol. 4, no. 6, pp. 185-194, 2015.

[11] J. M. Chang, T. Po-Chun, W. G. Isaac, C. C. Han, and C. F. Lai, ”Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach,” IEEE Systems Journal, vol. 9, no. 6, pp. 65-75, 2015.

[12] P. G. Fernando, M. C. A. Rossana, T. O. Carina, and J. N. Souza, ”EPMOSt: An energy-efficient passive monitoring system for wireless sensor networks,” Sensors, vol. 14, no. 3, pp. 10804-10828, 2015.

[13] X. Du, and H. Chen, ”Security in Wireless Sensor Networks,” IEEE Wireless Communications, vol. 15, no. 4, 2008.

[14] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ”A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet of Things Journal, vol. PP, no. 99, pp. 1-18, 2017.

[15] Z. Liu, X. Yang, P. Zhao, and W. Yu, ”On Energy-balanced Backpressure Routing Mechanisms for Stochastic Energy Harvesting Wireless Sensor Networks,” International Journal of Distributed Sensor Networks (IJDSN), vol. 12, no. 8, pp. 1-9, 2016.

[16] N. Hidehisa, K. Satoshi, J. Abbas, N. Yoshiaki, and K. Nei, ”A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks,” IEEE Transactions on Vehicular Technology, vol. 58, no. 13, pp. 2471- 2481, 2009.

[17] Y. X. Liu, M. X. Dong, O. Kaoru, and A. F. Liu, ”ActiveTrust: Secure and trustable routing in wireless sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 2013-2027, 2016.

[18] L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, ”An accurate and precise malicious node exclusion mechanism for ad hoc networks, "Ad Hoc Networks, vol. 19, no. 6, pp. 142-155, 2014. S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y Nemoto,

[19] ”Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method,” International Journal of Network Security, vol. 5, no. 9, pp. 14-21, 2007.

[20] D. Zhu, X. Yang, W. Yu, and X. Fu, ”Network Coding vs. Traditional Routing in Adversarial Wireless Networks,” International Journal of AdHoc Network-Elsevier, vol. 20, no. 2, pp. 119-131, 2014.