



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Active Trust Secure and Trustable Routing in Wireless Ad-hoc Networks

T.Arivanantham¹, Rahul Karmore², Nikita Satkar³, Priyanka Ghadge⁴, Karishma Shete⁵

Associate Professor, Department of Computer Engineering, D.Y.Patil College, Pimpri, Pune, Maharashtra, India¹

B.E. Student, Department of Computer Engineering, D.Y.Patil College, Pimpri, Pune, Maharashtra, India²

B.E. Student, Department of Computer Engineering, D.Y.Patil College, Pimpri, Pune, Maharashtra, India³

B.E. Student, Department of Computer Engineering, D.Y.Patil College, Pimpri, Pune, Maharashtra, India⁴

B.E. Student, Department of Computer Engineering, D.Y.Patil College, Pimpri, Pune, Maharashtra, India⁵

ABSTRACT: Wireless Ad-Hoc Network is increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks. To conquer that challenge, an active detection-based security and trust routing scheme named ActiveTrust is proposed for Wireless Ad-Hoc Network. In the proposed trust management scheme, the trust model has two components: trust from direct observation and trust from indirect observation. For this we are using three types of technique i.e. Initial Bait, Reverse trace request and reverse trace status, Dynamic threshold. The system resolves the problem of packet loss, forwarding packet in network and also resolve the problem of discarded packets. Combining these two components in the trust model, we can obtain more accurate trust values of the observed nodes in Wireless Ad-Hoc Network. Evaluating our scheme under the scenario of WSN routing is also done. The number of nodes used as an intermediary can also be reduced by using packet forwarding and also check the dummy packet.

KEYWORDS: Routing, Cooperation, Reputation ,Mobile Ad-hoc Networks ,Fairness ,Robustness ,Trust

I. INTRODUCTION

Wireless Ad-Hoc Network are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, military and civilian domains. Due to economic considerations, the nodes are usually simple and low cost. They are often unattended, however, and are hence likely to suffer from different types of novel attacks. The Wireless Ad-Hoc Network is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors.

A Wireless Ad-Hoc Network is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. Wireless Ad-Hoc Network are regarded as a revolutionary information gathering method to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. Compared with the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, Wireless Ad-Hoc Network will become the key technology.

II. RELATED WORK

Author[1] aiming at the serious impact of the typical network attacks caused by the limited energy and the poor deployment environment of wireless sensor network (wsn) on data transmission, a trust sensing-based secure routing mechanism (tssrm) with the lightweight characteristics and the ability to resist many common attacks simultaneously is proposed in this paper, at the same time the security route selection algorithm is also optimized by taking trust degree and qos metrics into account. Performance analysis and simulation results show that tssrm can improve the security and effectiveness of wsn .Author[2] security problems have become obstacles in the practical application of wireless sensor



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

networks (wsns), and intrusion detection is the second line of defense. In this work, an intrusion detection based on dynamic state context and hierarchical trust in wsns (idsht) is proposed, which is flexible and suitable for constantly changing wsns characterized by changes in the perceptual environment, transitions of states of nodes and variations in trust value. A multidimensional two-tier hierarchical trust mechanism in the level of sensor nodes (sns) and cluster heads (chs) considering interactive trust, honesty trust and content trust is put forward, which combines direct evaluation and feedback-based evaluation in the fixed hop range. This means that the trust of sns is evaluated by chs, and the trust of chs is evaluated by neighbour chs and bs; in this way, the complexity of evaluation is reduced without evaluations by all other chs in networks. Meanwhile, the intrusion detection mechanism based on a self-adaptive dynamic trust threshold is described, which improves the flexibility and applicability and is suitable for cluster-based wsns..Author[3] monitoring systems are important for debugging and analysing wireless sensor networks (wsn). In passive monitoring, a monitoring network needs to be deployed in addition to the network to be monitored, named the target network. The monitoring network captures and analyzes packets transmitted by the target network. An energy-efficient passive monitoring system is necessary when we need to monitor a wsn in a real scenario because the lifetime of the monitoring network is extended and, consequently, the target network benefits from the monitoring for a longer time. In this work, we have identified, analyzed and compared the main passive monitoring systems proposed for wsn. During our research, we did not identify any passive monitoring system for wsn that aims to reduce the energy consumption of the monitoring network. Therefore, we propose an energy-efficient passive monitoring system for wsn named epmost that provides monitoring information using a simple network management protocol (snmp) agent. Thus, any management tool that supports the snmp protocol can be integrated with this monitoring system. Experiments with real sensors were performed in several scenarios

III. PROPOSED ALGORITHM

Let S contains the set $S=\{IP, PRO, OP\}$

A. IP={Input}

Let 'W' be the set of whole system which contains

$W= \{RREP, RREQ', P, T, S, K, K'\}$.

Where,

1. RREP = Reply message.
2. RREQ' = message sent when attack occurred at some node.
3. P is the set of number of nodes in the network.
 $P=\{n1, \dots, nk, \dots, nm, \dots, nr\}$.
4. T is set of trusted nodes.

B. PRO={Procedure}

Step 1: Initial Bait.

Step 2: Initial Reverse Tracing.

Step 3: Dynamic Threshold.

1. Initial Bait:

- The goal of the bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ that it has used to advertise itself as having the shortest path to the node that detains the packets that were converted.
- To achieve this goal, the following method is designed to generate the destination address of the bait RREQ .The source node stochastically selects an adjacent node, within its one-hop neighborhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ.
- First, if the neighbor node had not launched a black hole attack, then after the source node had sent out the RREQ , there would be other nodes' reply RREP in addition to that of the neighbor node. This indicates that the malicious node existed in the reply routing.

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

- The reverse tracing program in the next step would be initiated in order to detect this route. If only the neighbor node had sent the reply RREP, it means that there was no other malicious node present in the network and that the system had initiated the DSR route discovery phase.

2. Initial Reverse Tracing:

- The reverse tracing program is used to detect the behaviors of malicious nodes through the route reply to the RREQ message.
- If a malicious node has received the RREQ, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route.
- It should be emphasized that the system is able to detect more than one malicious node simultaneously when these nodes send reply RREPs.

3. Dynamic Threshold:

- When the route is established and if at the destination it is found that the packet delivery ratio significantly falls to the threshold, the detection scheme would be triggered again to detect for continuous maintenance and real-time reaction efficiency.
- After Reverse Trace Request if the intermediate node requests for more than threshold request (i.e. two or more than two) then it will consider as malicious.

C. OP={Output}

Secure communication with trusted network.

IV. IMPLEMENTATION.

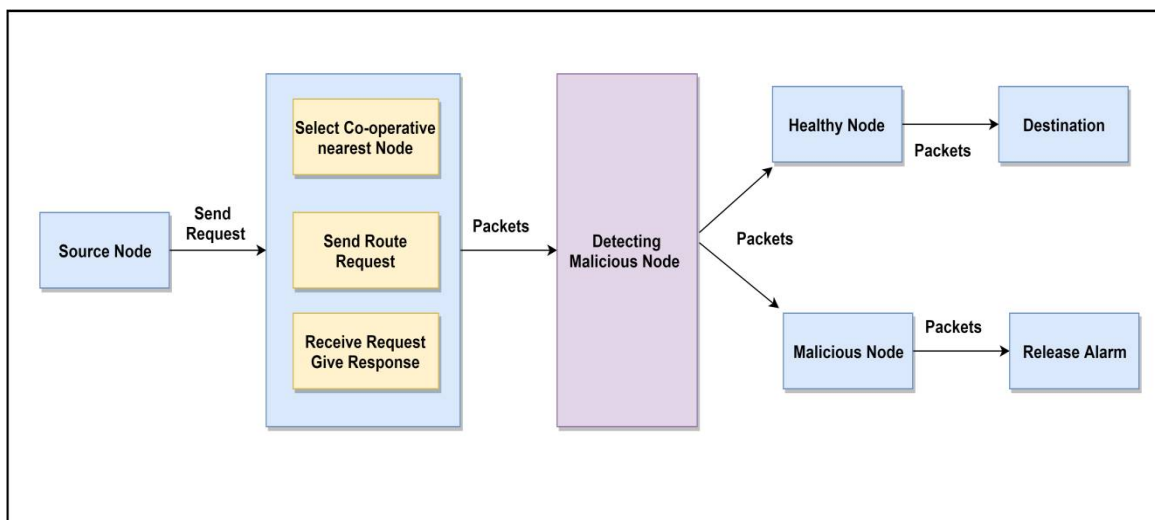


Figure i: Architecture of the proposed system.

International Journal of Innovative Research in Computer and Communication Engineering

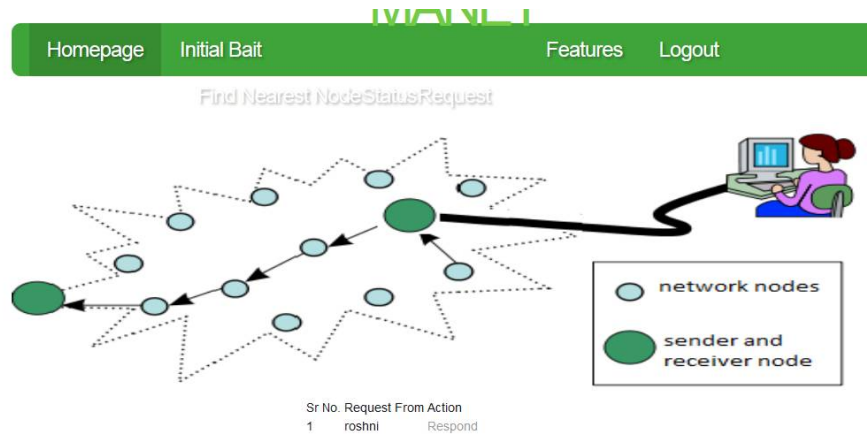
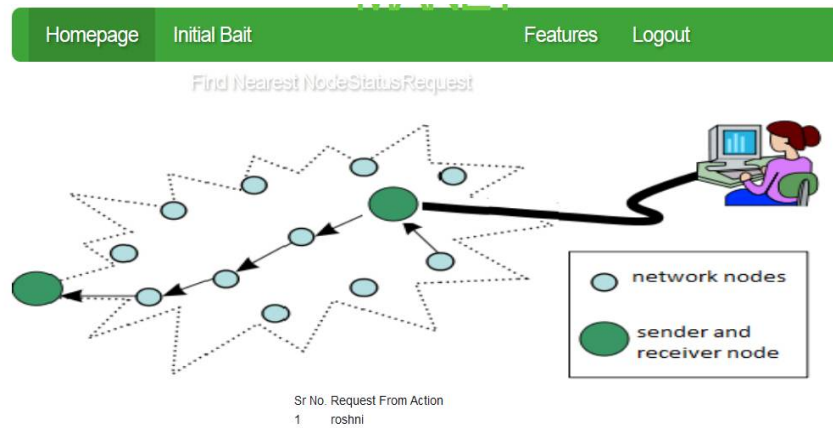
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

V. SIMULATION RESULTS

We propose a unified Active Trust management scheme that enhances the security in Wireless Sensor Network. In the proposed scheme, the trust model has two components: trust from direct observation and trust from indirect observation. For this we are using three types of technique i.e. Initial Bait, Reverse trace request and reverse trace status, Dynamic threshold. The system resolves the problem of packet loss, forwarding packet in network and also resolve the problem of discarded packets.



International Journal of Innovative Research in Computer and Communication Engineering

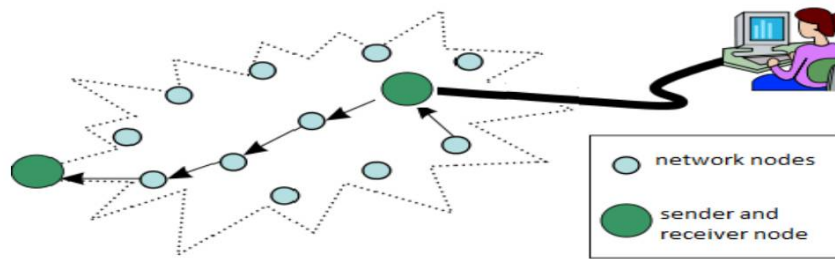
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

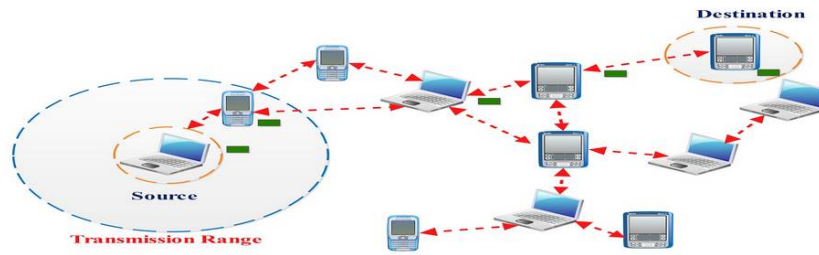
Reverse Trace Features Logout

Reverse Trace Status Reverse Trace Request



Sr No.	Node Name	Request	Action
1	roshni	Active	
2	rahul	Active	
3	ss	Active	

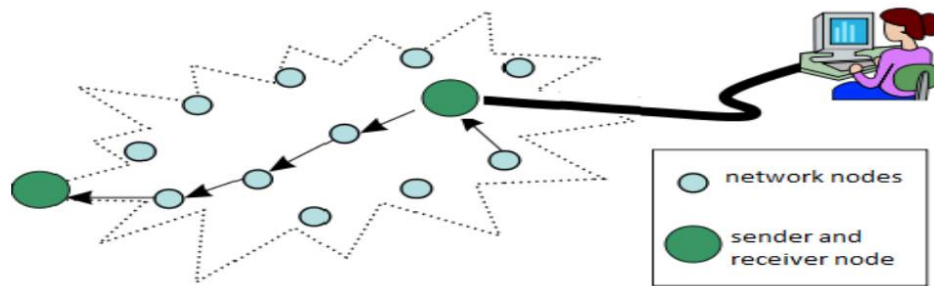
Homepage Node About project Features



Username :

Password :

Homepage Initial Bait Reverse Trace Features Logout



Sr No.	Node Name	Request	Action
1	roshni	Malicious	Time out to respond
2	oo	Malicious	Time out to respond

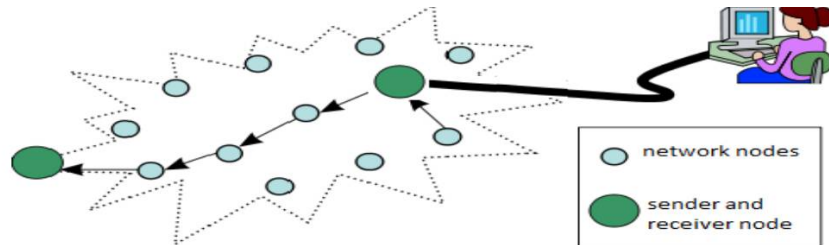


International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018



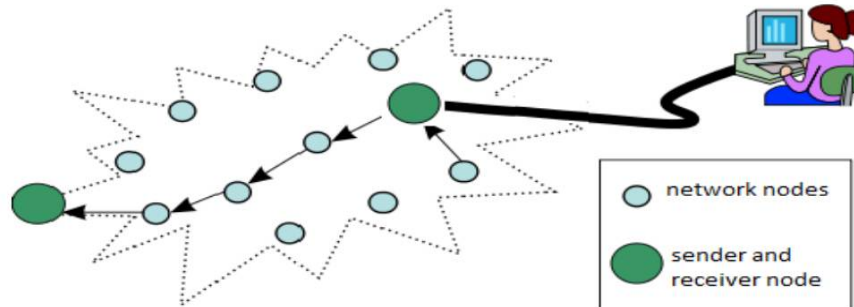
My Bandwidth : 2000

Nearest Nodes

Sr No.	Username	Range
1	oo	4000
2	roshni	3000

Send Initial Request

[Homepage](#) [Initial Bait](#) [Reverse Trace](#) [Routing](#) [Logout](#)



My Bandwidth : 2000

Select :

[Homepage](#) [Node](#) [About project](#) [Features](#)

Node Name :

Hostname :

IP Address :

Username :

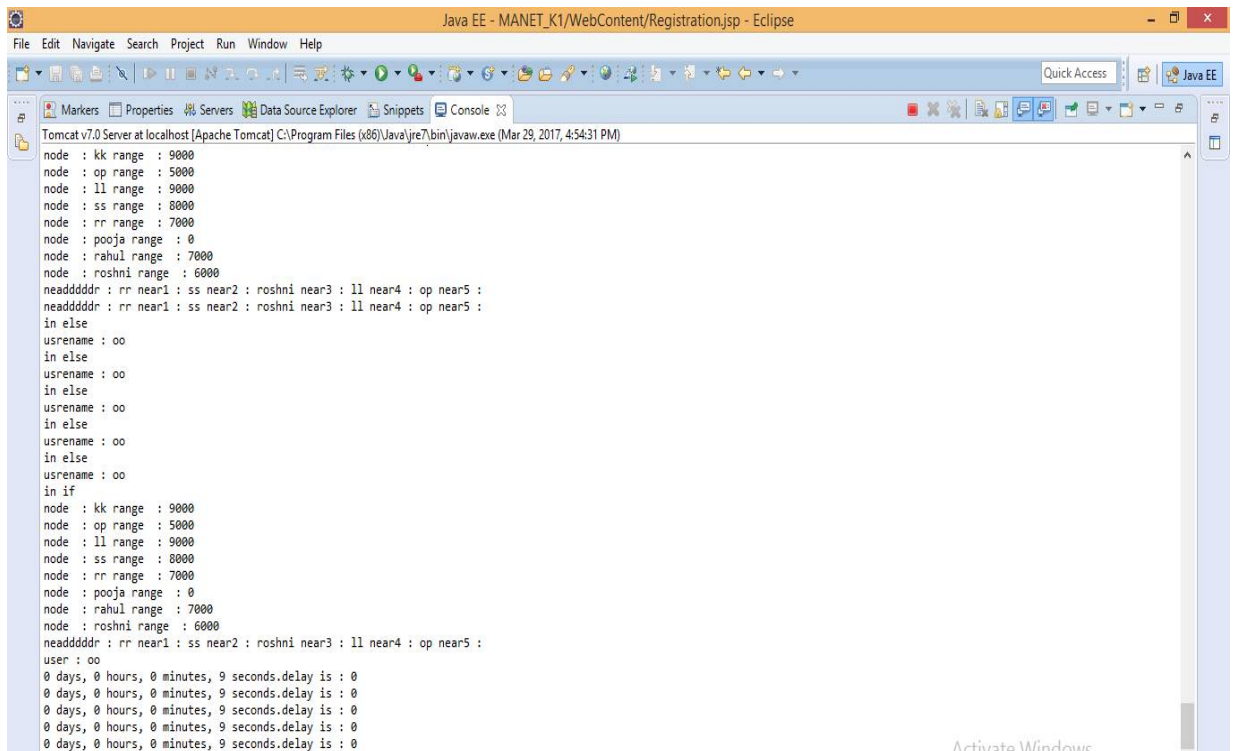
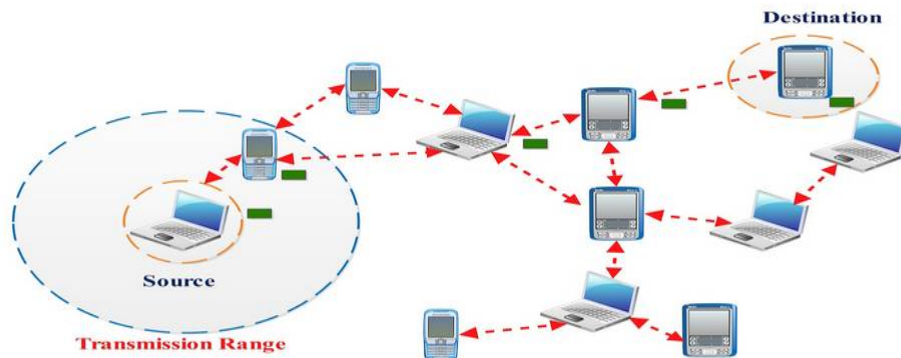
Password :

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018



VI. CONCLUSION AND FUTURE WORK

An Active Trust model is introduced to enhance the security in wireless sensor networks that includes direct and indirect observation. For this we are using three types of technique i.e. Initial Bait, Reverse trace request and reverse trace status, Dynamic threshold. The system resolves the problem of packet loss, forwarding packet in network and also resolve the problem of discarded packets. It registers each node needed for data transmission and sends the data. It ensures a secure transmission. It provides a trustful network.



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijirccce.com

Vol. 6, Issue 5, May 2018

REFERENCES

- [1] S. Corson and J. Macker, Mobile Ad Hoc Networking (MANET): Routing protocol performance issues and evaluation considerations, Jan. 1999, IETF RFC 2501.
- [2] F. R. Yu, *Cognitive Radio Mobile Ad Hoc Networks*. New York, NY, USA: Springer-Verlag, 2011.
- [3] J. Loo, J. Lloret, and J. H. Ortiz, *Mobile Ad Hoc Networks: Current Status and Future Trends*. Boca Raton, FL, USA: CRC, 2011.
- [4] Q. Guan, F. R. Yu, S. Jiang, and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," *IEEE Trans. Veh. Tech.*, vol. 61, no. 6, pp. 2674–2685, Jul. 2012.
- [5] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and Quality of Service (QoS) co-design in cooperative mobile ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, pp. 188–190, Jul. 2013.
- [6] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1616–1627, Mar. 2014.
- [7] J. Chapin and V.W. Chan, "The next 10 years of DoD wireless networking research," in *Proc. IEEE Milcom*, Nov. 2011, pp. 2155–2245.
- [8] S. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 3, pp. 1025–1036, Mar. 2011.