Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 6, June-2018

Active Trust: Secure and Trustable Routing in WSN

Amol Dhakne, Amitaakole, Aishwarya Gupta,Kiran bhadekar, Karnawat Shradhha

dhakne.amol5@gmail.com,amitaakole@gmail.com, aishwaryagupta232@gmail.com,
kiran.rbhadekar@gmail.com, karnawatshraddha96@gmail.com

D.Y.Patil College Of Engineering,Department Of Computer Technology,Pune

Abstract — WAN is remaining arranged in security-critical requests. Due to their inherent resource-constrained characteristics, they are given to various security attacks. To overcome that challenge, an active detection-based security and trust routing scheme named Active Trust is proposed for Wireless Ad-hoc Network. The designed trust management system trust model has two mechanisms: trust from direct observation and trust from indirect observation. Just for this we are using three forms of technique i.e. Initial Bait, Reverse trace request and reverse trace status, Dynamic threshold. The device resolves the issue of packet loss, forwarding packet in network as well as resolve the situation of discarded packets. Combining these two components within the trust model, we can easily obtain better trust values of the observed nodes in Wireless Ad-hoc Network. Evaluating our scheme beneath the scenario of Wireless Ad-hoc Network routing is additionally done. The amount of nodes utilized as a middleman can also be reduced by making use of packet forwarding as well as check the dummy packet.

I. INTRODUCTION

Wireless Ad-hoc Network area unit rising as a promising technology thanks to their big selection of applications in industrial, environmental observance, military and civilian domains. because of economic issues, the nodes area unit sometimes straightforward and low value. they're usually unattended, however, and area unit thence doubtless to suffer from differing types of novel attacks. The Wireless Ad-hoc Network is constructed of "nodes" – from some to many lots of or maybe thousands, wherever every node is connected to at least one (or generally several) sensors. A Wireless Ad-hoc Network may be a network fashioned by an oversized range of device nodes wherever every node is provided with a device to notice physical phenomena like light-weight, heat, pressure, etc. Wireless Ad-hoc Network area unit thought to be a revolutionary operation methodology to create the knowledge and communication system which is able to greatly improve the dependableness and potency of infrastructure systems. Compared with the wired resolution, Wireless Ad-hoc Network feature easier readying and higher flexibility of devices. With the speedy technological development of sensors, Wireless Ad-hoc Network can become the key technology.

II. LITERATURE REVIEW

1. Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network

Authors: DANYANG QIN, SONGXIANG YANG, SHUANG JIA, YAN ZHANG, JINGYA MA, AND QUN DING

Description: 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 toresist many common attacks simultaneously is proposed in this paper, at the same time the security routeselection algorithm is also optimized by taking trust degree and

QoS metrics into account. Performanceanalysis and simulation results show that TSSRM can improve the security and effectiveness of WSN.

2. Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks

Authors: Zhihua Zhang, Hongliang Zhu, ShoushanLuo, Yang Xin and Xiaoming Liu

Description: Security problems have become obstacles in the practical application of wireless sensor 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 neighbor 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.

3. EPMOSt: An Energy-Efficient Passive Monitoring System for Wireless Sensor Networks

Authors: Fernando P. Garcia, Rossana M. C. Andrade, Carina T. Oliveira and

José Neuman de Souza

Description: Monitoring systems are important for debugging and analyzing Wireless SensorNetworks (WSN). In passive monitoring, a monitoring network needs to be deployed in addition to the network to be monitored, named the target network. The monitoringnetwork captures and analyzes packets transmitted by the target network. An energy-efficientpassive monitoring system is necessary when we need to monitor a WSN in a real scenariobecause the lifetime of the monitoring network is extended and, consequently, the targetnetwork 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. Duringour research, we did not identify any passive monitoring system for WSN that aims toreduce the energy consumption of the monitoring network. Therefore, we propose anEnergy-efficient Passive MOnitoringSysTem for WSN named EPMOSt that providesmonitoring information using a Simple Network Management Protocol (SNMP) agent.Thus, any management tool that supports the SNMP protocol can be integrated with thismonitoring system. Experiments with real sensors were performed in several scenarios.The results obtained show the energy efficiency of the proposed monitoring system and theviability of using it to monitor WSN in real scenarios.

4. A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks

Authors: Yanwei Wang, F. Richard Yu,Helen Tang,Minyi Huang

Description: Game theory can provide a useful tool to study the security problem in mobile ad hoc networks (MANETs). Mostof existing works on applying game theories to security only

consider two players in the security game model: an attackerand a defender. While this assumption may be valid for anetwork with centralized administration, it is not realistic in

MANETs, where centralized administration is not available. Inthis paper, using recent advances in mean field game theory, wepropose a novel game theoretic approach with multiple players for security in MANETs. The mean field game

theory providesa powerful mathematical tool for problems with a large numberof players. The proposed scheme can enable an individual node in MANETs to make strategic security defence decisions withoutcentralized administration. In addition, since security defencemechanisms consume precious system resources (e.g., energy), theproposed scheme considers not only the security requirement ofMANETs but also the system resources. Moreover, each node inthe proposed scheme only needs to know its own state informationand the aggregate effect of the other nodes in the MANET.Therefore, the proposed scheme is a fully distributed scheme.

5. Distributed Trust based Intrusion Detection Approach in Wireless Sensor Network

Authors: Amol R. Dhakne, Dr. P.N. Chatur

Description: Security of wireless sensor network is always a major thing as it has widespread application in most of the major domains such as battlefield surveillance, healthcare, etc. Basically there are three main components that deal with security of wireless sensor network, prevention, detection and mitigation. But it is very difficult to prevent wireless sensor network always from malicious attacks so it is always important to detect them as early as possible so that we can react to the attack not harm to wireless sensor network., This paper proposes Distributed Trust based Intrusion Detection (DTBID) approach which considers several factors for establishing trust of sensor node. Most of the research work only considers the communication behavior to derive the trust. Our intrusion detection system will consider trust which is distributed among some other factors such as energy, reliability, data etc. We derive and formulate trust such as direct trust, recommendation trust, and indirect trust from these factors. We provide an approach to decide whether particular node is malicious node or not by comparing subjective trust derived from our intrusion detection technique to that of objective trust which is calculated based on the actual information of each node without considering any network dynamics such as node mobility, trust decay over time, and any malicious attacks. If there is a lot of difference between subjective trust derived from our model to that of objective trust then we consider sensor node as malicious node.

6. Context-Aware Quality of Service in Wireless Sensor Networks

Authors: SudipMisra, Sankar Narayan Das, and Mohammad S. Obaidat

Description: In wireless sensor networks, densely deployed and resource-constrained sensor nodes observe their surroundings and communicate the sensed data to the sink. However, those observations are correlated — spatially and temporally. Furthermore, the communicated data, depending on their priority, require differentiated QoS, such as end-to-end delay and jitter. In this work, we use context awareness as a means of sharing information required to control the network, and providing differentiated QoS to the nodes and their transmitted data by exploiting spatial and temporal correlation. Simulation results show that context awareness helps nodes to manage the network in an energy-efficient manner.

III. EXISTING SYSTEM

Wireless Sensor Networks (WSNs) are proving to be a good technology due to their wide range of applications in industrial, environmental monitoring, military and civilian domains. The present trust-based route strategies face some challenging issues. (1) The core of your trust route is in obtaining trust. However, getting the trust of a node is quite difficult, and just how easy it really is is still unclear. (2) Energy efficiency. Because energy is quite limited in WSNs, generally in most research, the trust acquisition and diffusion have high energy consumption, which seriously affects the

network lifetime. (3) Security. Because it's challenging to locate malicious nodes, the safety route remains to be a frightening issue.

3.1 Disadvantages of Existing System

- Not secure.
- Performance is low.
- It cannot forwards packets securely in network.
- Obtaining the trust of a node is very difficult.
- Difficult to locate malicious nodes.

IV. PROPOSED SYSTEM

We propose a unified Active Trust management scheme that raises the security in Wireless Ad-hoc Network. From the proposed scheme, the trust model has two components: trust from direct observation and trust from indirect observation. Because of this we're using three kinds of technique i.e. Initial Bait also Reverse trace request and reverse trace status, Dynamic threshold. The machine resolves the situation of packet loss, forwarding packet in network and also resolve the challenge of discarded packets.

4.1 Advantages of Proposed System

- The designed presented structure distinguishes data packets and control packets, and meanwhile excludes the other causes that result in dropping packets, such as unreliable wireless connections and buffer overflows.
- It is more secure.
- It detects the all malicious node.
- It's a trustful network.
- Forward packet without dropping the data.

V. SYSTEM ARCHITECTURE

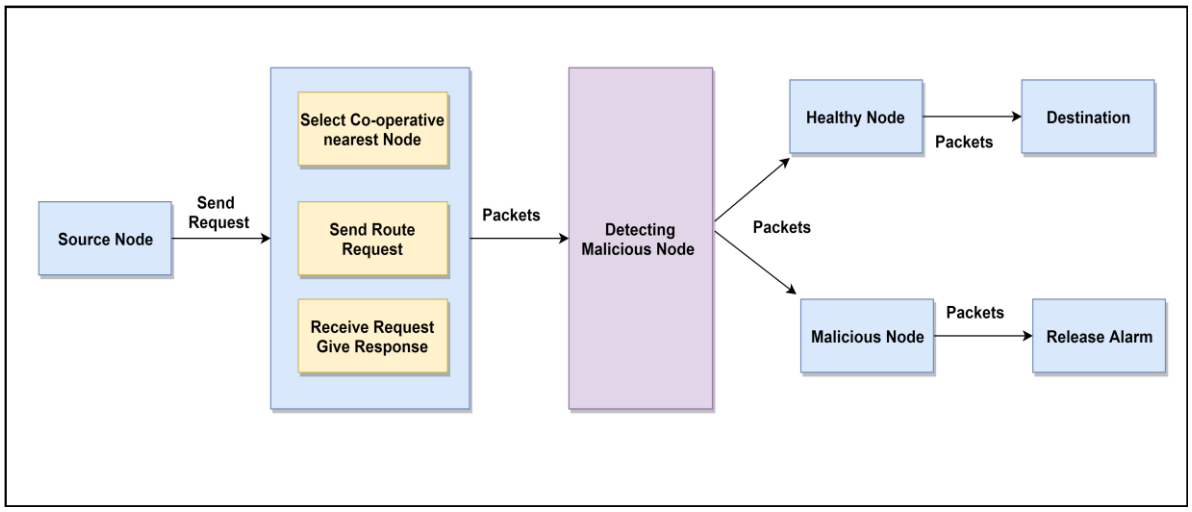


Figure 1. Proposed System Architecture

VI. ALGORITHM

1: Initial Bait

The goal of the bait phase is to entice a malicious node to send a reply RREPby 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 adjacentnode, within its one-hop neighborhood nodes and cooperates with this nodeby taking its address as the destination address of the bait RREQ. First, ifthe neighbor node had not launched a black hole attack, then after the sourcenode had sent out the RREQ , there would be other nodes reply RREP inaddition to that of the neighbor node. This indicates that the maliciousnode existed in the reply routing. The reverse tracing program in the nextstep 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 maliciousnode present in the network and that the CBDA had initiated the DSR route discovery phase.

2: Initial Reverse Tracing

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

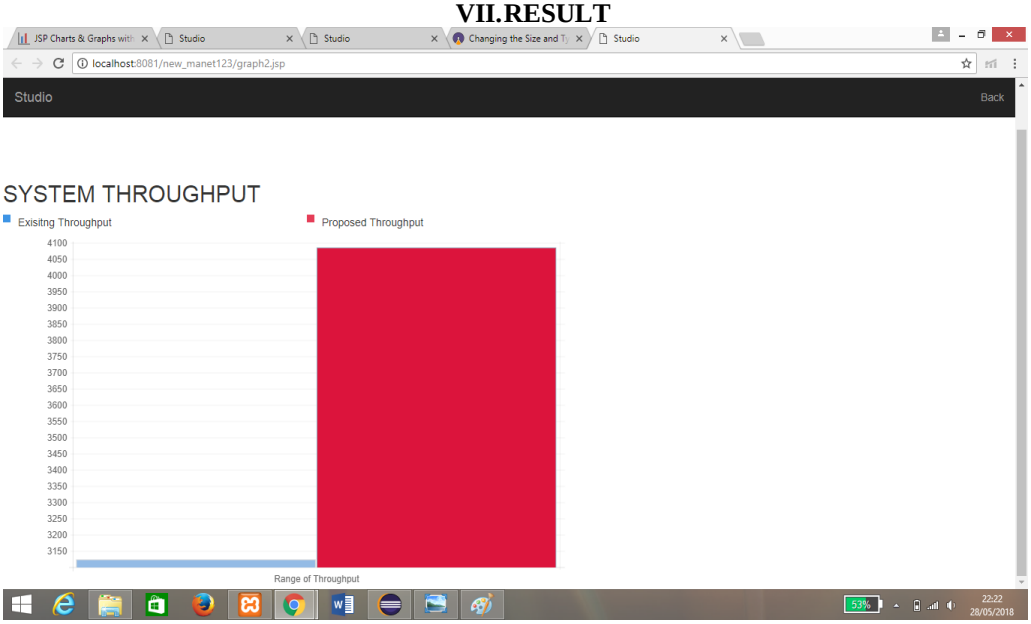
3: Dynamic Threshold

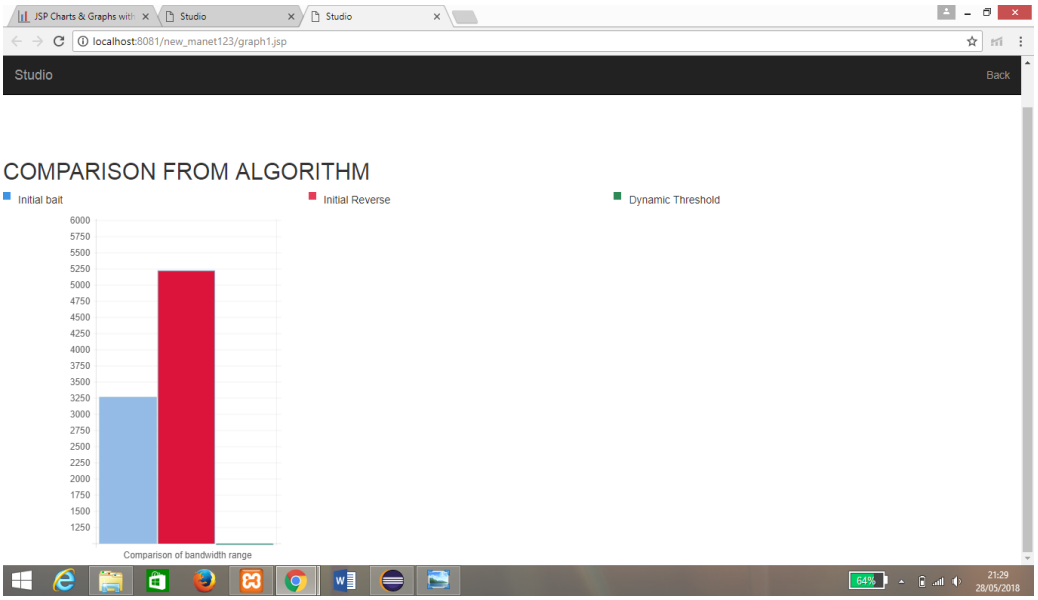
When the route is established and if at the destination it is found that the packet delivery ratio significantly falls to the threshold, the detection schemewould be triggered again to detect for continuous maintenance and real-time reaction efficiency. The threshold is a varying value in the range thenthe packet delivery ratio falls under the same threshold. If the descendingtime is shortened, it means that the malicious nodes are still present in thenetwork. In that case, the threshold should be adjusted upward. Otherwise,the threshold will be lowered.

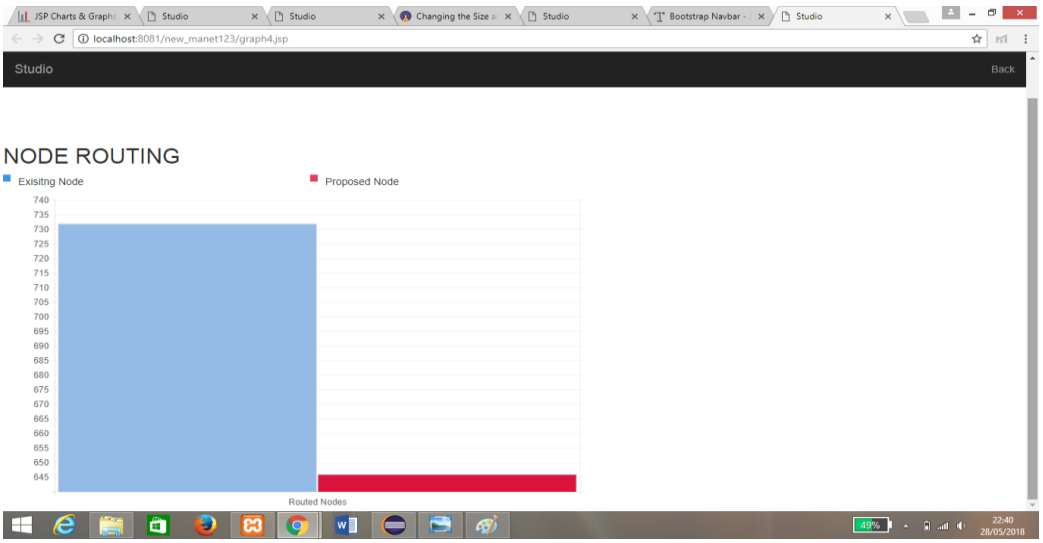
4: Security Module

It is going to use the as key value of the message which is going to be sent andthen it is added with the public key and sent from the source to destinationthrough the intermediate node and then decrypted in the destination bysubtracting the public key from the message obtained and then the originalmessage is obtained from the packets sent.

VII.RESULT







VIII. CONCLUSION AND FUTURE SCOPE

An ActiveTrust model is brought to enhance the reassurance of wireless sensor networks that includes indirect and direct observation. Because of this we have been using three varieties of technique i.e. Initial Bait, Reverse trace request and reverse trace status, Dynamic threshold. The device resolves the problem of packet loss, forwarding packet in network as well as resolve the issue of discarded packets. It registers each node needed for data transmission and sends the data. It ensures a secure transmission. It possesses a trustful network.

REFERENCES

[1] Qin, Danyang, et al. "Research on Trust Sensing based Secure Routing Mechanism for Wireless Sensor Network." *IEEE Access* (2017).

[2] Zhang, Zhihua, et al. "Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks." *IEEE Access* 5 (2017): 12088-12102.

[3] Fernando P. Garcia, Rossana M. C. Andrade, Carina T. Oliveira and José Neuman de Souza "An Energy-Efficient Passive Monitoring System for Wireless Sensor Networks" *IEEE Access* 5 (2017): 12088-12103.

[4] Yanwei Wang, F. Richard Yu,Helen Tang,Minyi Huang "Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks" 4.3 (2008): 15

[5] Amol R. Dhakne, Dr. P.N. Chatur "Distributed Trust based Intrusion Detection Approach in Wireless Sensor Network" 2010-MILCOM 2010. IEEE, 2010

[6] SudipMisra, Sankar Narayan Das, and Mohammad S. Obaidat "Context-Aware Quality of Service in Wireless Sensor Networks" 10.9 (2011): 3064-3073.

[7]Changiz, Reyhaneh, et al. "Trust establishment in cooperative wireless networks." MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010. IEEE, 2010.

[8] Bu, Shengrong, et al. "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks." IEEE Transactions on Wireless Communications 10.9 (2011): 3064-3073.

[9] Ganeriwal, Saurabh, Laura K. Balzano, and Mani B. Srivastava. "Reputation-based framework for high integrity sensor networks." ACM Transactions on Sensor Networks (TOSN) 4.3 (2008): 15.