European Journal of Applied Sciences 8 (1): 55-61, 2016
ISSN 2079-2077

DOI: 10.5829/idosi.ejas.2016.8.1.22863

Quadratic Route Factor Estimation Technique for Routing Attack Detection in Wireless Adhoc Networks

[1]K. Jayarajan and [2]A. Sabari

[1]Research scholar, Anna University, Chennai, Tamil Nadu, India
[2]Department of Information Technology,
K.S.Rangasamy College of Technology, Tiruchengode, Tamil Nadu, India

Abstract: The modern wireless adhoc networks has more impact of routing attacks due to the topology changes and the problem of routing attack detection has been performed in number of approaches. The earlier methods suffer with the problem of poor detection accuracy and the performance of mitigation approaches. To overcome the issue of routing attack detection, an novel quadratic route factor estimation technique has been proposed in this paper. The method maintains route details and network information at each time frame based on different quarters of geographic network region. The method splits the region of entire network into four quarters and for each quadratic region, a time based snapshot and route details are stored. Based on the route trace and snapshot of the network the routing attack is mitigated in different locations of the entire network. The method selects a few set of nodes in the network to perform the detection of routing attack where the selection of node is performed based on various parameters. The distributed detection of routing attack increases the performance of the network and improves the throughput ratio also. Similarly for the detection of routing attack, the method uses the snapshot and route traces with the help of packet information.

Key words: Wireless Adhoc Networks · Quadratic Route Factor · Routing Attacks · Sink Hole Attack · Botnet Attacks

INTRODUCTION

The modern wireless adhoc network is the collection of number of wireless devices moving across the geographic region of the network. There are numbers of services the users of the network accessing and the user is able to move throughout the network and could access the services from anywhere in the network. The mobility of the wireless nodes makes the topology of the network to change and the routing in the network is performed in collaborative manner where all the nodes participate in routing of packets. The mobility of the network makes the topology to change at each time window and from the topology being identified the method can obtain the number of routes available in the network.

The entire region of the network can be split into regions and by splitting the region of the network into four quarters, the network can be split into four numbers. For each quadratic region, there will be number of nodes and there exists more number of routes to reach the sink node of the network. The required service may be available in any node present in the network, in order to access the service the service request has to be moved from the source node to the sink node where the service is available. To deliver the request from the source node to the destined node, the route request packet has to be routed in the network. The request packet can be transferred through any route and for each route in the network, the route factor can be computed.

The route factor is the value which represents the trustworthy of the route in transmitting the packet towards the sink node. The route factor can be computed according to the packet information like the number of packets being transmitted in any time window, the payload of packets, the number of nodes present in the route and their participation in routing attack and so on. Based on the route factor the routes trustworthy can be computed and helps identifying the presence of malicious nodes in the route.

Corresponding Author: K. Jayarajan, Research scholar, Anna University, Chennai, Tamil Nadu, India.

The routing of packets in any network has the threat of different attacks and one among them is the routing attack. The routing attack includes generation of sink holes, longest route forwarding, eaves dropping of packets and many more. The sink hole attack is one which generates a hole around the sink node and makes the routes unusable through the node. This reduces the number of routes to be reduced which increases traffic in other routes and makes the other nodes to suffer with energy. Incase of longest route forwarding attack, the malicious nodes choose the longest route even there exist shortest routes to reach the destination, which reduces the energy of entire nodes of the network. In eaves dropping attack, the malicious node drops the packet blindly. This paper considers the above mentioned attacks and how they can be mitigated using the proposed approach.

Related Works: There are number of methods has been discussed for the mitigation of routing attacks in wireless adhoc networks and this section discusses about few methods discussed earlier.

Detection of wormhole attacks in wireless sensor networks using range-free localization [1], propose two wormhole detection procedures for WSNs, based on concepts employed in a kind of range-free localization methods: one of the approaches performs the detection simultaneously with the localization procedure and the other operates after the conclusion of the location discovery protocol. Both strategies are effective in detecting wormhole attacks, but their performance is fairly sensitive to shadowing effects present in the radio channels.

Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool [2], uses a sequence number based sinkhole detection approach. The sender node first requests the sequence number with the rreq message, if the node replies its sequence number with rrep message. Transmitting node will match sequence number in its routing table. If matches then data will be shared otherwise it will be assign the sequence number to the node. If the node accepts the sequence number then the node will enter in the network otherwise it will be eradicated from the network.

Intrusion detection of sinkhole attacks in large-scale wireless sensor networks [3], proposes a novel algorithm for detecting sinkhole attacks for large-scale wireless sensor networks. We formulate the detection problem as a change-point detection problem. Specifically, we monitor the CPU usage of each sensor node and analyze the consistency of the CPU usage. Thus, the proposed algorithm is able to differentiate between the malicious and the legitimate nodes.

A sinkhole attack detection scheme in Mintroute wireless Sensor Networks [4], where the vulnerabilities of Mintroute protocol to sinkhole attacks are discussed and the existing manual rules used for detection are investigated using different architecture.

Network Forensics using JADE [5-9], is proposed by Asha Nagesh for the detection of denial of service attacks. It captures the underlying network packets and hands that are to the popular intrusion detection system. Snort has used the intrusion detection system and functions with the support of rule set provided. The framework is used to find out the attacks carried out and the signature of the packets. The purpose is to improve the intrusion detection system and provide support to the network administrator. It analyzes the packets to find out the attack using predefined rules, so that new kind of attacks cannot be identified.

Host Based intrusion Detection system [10] presented an intrusion detection system which informs system administrator about potential intrusion incidence in a system. The designed architecture employs statistical method of data evaluation that allows detection based on the knowledge of user activity deviation in the computer system from learned profile representing standard user behavior.

Network intrusion detection system NID [11], is designed as a data mining framework to automatically detect attacks against computer networks and systems. An unsupervised anomaly detection technique assigns a score to each network connection that reflects how anomalous the connection is proposed with association pattern analysis module to summarize those network connections that are ranked highly anomalous by the anomaly detection module.

Network Intrusion Detection System [12] is proposed which embedded a NIDS in a smart-sensor-inspired device under a service-oriented architecture (SOA) approach. Using this embedded NIDS can operate independently as an anomaly-based NIDS, or integrated transparently in a Distributed Intrusion Detection System (DIDS). It combines the advantages of the smart sensor approach and the subsequent offering of the NIDS functionality as a service with the SOA use to achieve their integration with other DIDS components. It also addresses the construction of a physical sensor prototype. This prototype was used to carry out the tests that have demonstrated the proposal's validity, providing detection.

An Activity Pattern Based Wireless Intrusion Detection System [13] was designed for wireless network. It exploits pattern recognition techniques to model the usage patterns of authenticated users and uses it to detect intrusions in wireless networks. User activity is monitored and their discriminative features are extracted to identify intrusions in wireless networks. The detection module uses PCA technique to accumulate interested statistical variables and compares them with the thresholds derived from users' activities data. When the variables exceed the estimated thresholds, an alarm is raised to alert about a possible intrusion in the network. The novelty of the proposed system lies in its light-weight design which requires less processing and memory resources and it can be used in real-time environment.

We propose a quadratic route factor estimation technique based routing attack mitigation model to perform detection of various attacks in wireless adhoc networks and mitigation of them to develop the quality of service in wireless adhoc networks.

Quadratic Route Factor Model Based Routing Attack Detection: The quadratic route factor model splits the entire network region into four parts at 90 digress and for each quarter, the method maintains time orient snapshot which shows the network topology and from the topology being generated, the method computes the available routes to reach the sink node. Based on the topology and route information with the support of packet details the method computes route factor for each distinct route available in the network. The entire process can be split into number of stages namely time orient snapshot generation, route discovery, quadratic route factor estimation, Routing attack mitigation. Each stage of the proposed model will be discussed in detail in this section [14].

Time Orient Snapshot Generation: This section performs the capturing of network details and generates the topology of the network. The Time orient snapshot generation mechanism is performed by the sink node at each time window. The sink node maintains the traces of packets and the location details of the nodes in different region. Using the mentioned information, the sink node generates the network topology at each time window, because the mobility of the nodes makes the topology to change in frequent manner and to support the detection of routing attacks the requirement of network topology is essential. The generated snapshot will be updated with the quadratic routing attack detection nodes.

Algorithm:
Input: Node Details Nd, Route Table Rt
Output: Network Topology NT, Route Table Rt.
Start
Split region into four quarters.
Rs = $\int_{i=1}^{4} Region \times Split(i \times 90)$
for each region Ri from Rs
for each time window Ti
Identify Number of nodes present in the network region.
Nd = $\int \sum Nodes(Ri) \uparrow\downarrow Ri$
Generate topology Nt.
end
Stop.

The above discussed algorithm computes the network topology for each quadratic region being identified and will be used to perform route discovery.

Route Discovery: The route discovery is the process of computing available routes in each region topology. The time orient snapshot only generates the network structure and from the generated topology, the method computes the total number of routes available from the source node to reach the sink node. Once the number of distinct routes are identified then the method computes the hop count for each of the route available. The computed routes will be used to compute the quadratic route factor in the next stage.

Algorithm:
Input: Topology Set Ts
Output: Route Table Rt
Start
for each entry Ti from Ts
Identify the neighbors of source node Sn.
Ns = $\sum Neighbors(Ti, Sn) \forall TransmissionRange(Sn)$
Compute available routes through each neighbor.
for each neighbor Ni from Ns
compute routes available.
Rts = $\sum_{i=1}^{size(Ni.Neighbor)} Route \in Ti$
Add routes to Rt.
Rt = $\sum(Routes \in Rt) \cup Rts$
End
End
Stop.

The above discussed algorithm computes the available routes in each region to perform routing attack detection.

Quadratic Route Factor Estimation: The quadratic route factor is the value computed on each region according to the packet traces. The method maintains the traces of packets which has been transferred in any route and for each route the method compute the packet transfer rate, payload and hop count and so on. Based on the computed measures, the method computes the quadratic route factor which represents the routes trustworthy for the packet transfer. The method uses the malicious trace where it has stored number of packet traces which has been identified and based on the trace the method computes the QRF value.

Algorithm:
Input: Route Table Rt, Network Trace Nt.
Output: QRF value
Start
for each route Ri from Rt
Compute transmission frequency.
Tf = $\frac{\sum Traces.Ri \in Nt}{size(Nt.region)}$
Compute average payload.
APl = $\frac{\sum(Traces.Ri \in Nt).Payload}{size(Nt.region)}$
Compute average hop count AHC.
AHC = $\frac{\sum(Traces.Ri \in Nt).HC}{size(Nt.region)}$
Compute Common Hops present in malicious trace.
MCH = $\sum Hops(Traces.Ri \in MH) \forall MH$
Compute number of matches in MCH.
NM = $\sum Hops(Ri) \in MCH$
Compute QRF = $\frac{Tf \times APL}{AHC \times NM}$
End
Stop.

The above discussed algorithm computes the quadratic route factor for each of the route being identified in the previous section. The computed QRF value will be used to perform routing attack detection.

Routing attack Mitigation: The routing attack is detected and mitigated based on the value of quadratic route factor. The method computes the quadratic route factor for each route available and if there exist more than number of malicious routes then the method deploys a temporary sink node where the data will be collected and will perform routing attack detection. The method computes QRF value for each route and based on the value of QRF the method decides whether the route is trustworthy or not.

Algorithm:
Input: Route Table Nt
Output: Null
Start
    Initialize Malicious Routes MRS.
    for each region Ri from Rs
        for each time window Ti
            Generate Snapshot.
            Perform Route Discovery
            For each route R
                compute QRF.
                if QRF>RTh then
                        Add to MRS.
                        MRS = $\sum Routes(MRS) \cup Ri$
                End
            End
            if size(MRS) > ((1/3)×size(NT)) then
                Deploy Temporary sink node.
            End
            Choose least QRF valued route.
            Transmit packet on specific route.
    End
Stop.

The above discussed algorithm computes malicious routes and if the number of malicious routes are more than 1/3 rd of the available routes then the method deploys temporary sink on the region identified.

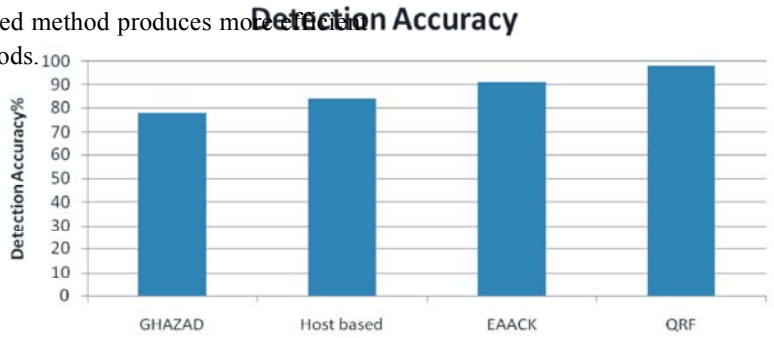
RESULTS AND DISCUSSION

The proposed Quadratic Route Factor Estimation Based network threat identification and mitigation model has been implemented in Network simulator NS2. We have designed network topology with different scenarios with different number of nodes. The proposed methodology has been evaluated with different density networks with multiple malicious nodes. The following Table 1 shows the simulation parameters used to evaluate the proposed method. NS-2 has written using C++ language and it uses Object Oriented Tool Command Language (OTCL). It came as an extension of Tool Command Language (TCL). The simulations were carried out using a WAN environment consisting of 71 wireless nodes over a simulation area of 1000 meters x 1000 meters flat space operating for 60 seconds of simulation time. The radio and IEEE 802.11 MAC layer models were used.

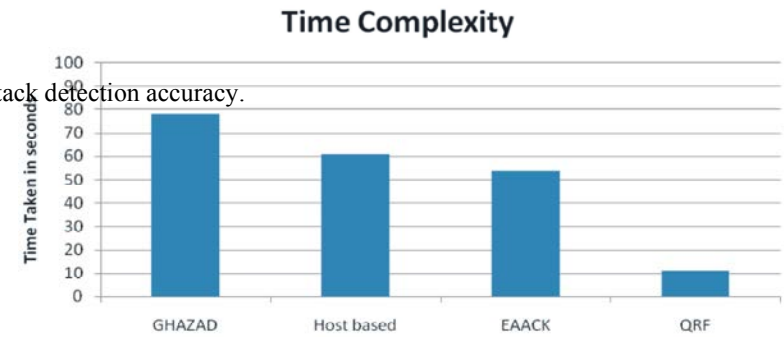
The Table 1, shows the details of simulation being used to evaluate the performance of the proposed method.

The Table 2, shows the result of comparative analysis of proposed method on different parameters. The result

shows that the proposed method produces more efficient result than other methods.



Graph1: shows the attack detection accuracy.



Graph 2: Comparison of time complexity

Table 1: The parameters used in our simulation

Parameters	Value
Version	NS-allinone 2.34
Protocols	QRF
Area	1000m x 1000m
Transmission Range	250 m
Traffic model	UDP,CBR
Packet size	512 bytes

Table 2: Shows the comparison results

			Detection Rate			
S.No	Number of Nodes	Protocol	False +ve	False-ve	Throughput	PDF
1.	100	GEOSTATICAL HAZARD MODEL	3.5	2.5	92	86.70
2	100	HOST BASED	3.2	2.3	94	89.50
3	100	EAACK	2.8	1.9	95	92.70
4	100	QRF	0.4	0.7	98.8	97.50

The Graph 1, shows the attack detection accuracy produced by different methods and it shows clearly that the proposed method has produced more accuracy in network threat identification.

The Graph 2 shows the comparison of time complexity produced by different methods and it shows clearly that the proposed method has produced less time complexity than other methods.

CONCLUSION

This paper discusses an efficient quadratic route factor estimation based routing attack mitigation approach for wireless adhoc networks. The method splits the entire geographic region into four quarters in the perspective of source node and for each region the method generates time orient snapshot and topology. From the topology being generated, the

method computes the available routes and then for each route the quadratic route factor is computed. Using the computed QRF value the method identifies the trustworthy of the node. Also if the number of routes in any region has more QRF value then the method deploys the temporary sink node in the region to perform attack detection. The deployment of temporary sink node increase the possibility of identifying the malicious packet with routing attack in the region itself and improves the performance of routing attack detection.

REFERENCES

1. Otero Garcia, 2012. Detection of wormhole attacks in wireless sensor networks using range-free localization, Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp: 21-25.
2. Singh Tejinderdeep, 2013. Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool, International Journal of Advanced Computer Science and Applications, 4(2).
3. Intrusion detection of sinkhole attacks in large-scale wireless sensor networks, 2010.Wireless Communications, Networking and Information Security (WCNIS), pp: 711-716.
4. Rassam, M.A., 2012. A sinkhole attack detection scheme in Mintroute wireless Sensor Networks, Telecommunication Technologies (ISTT), pp: 71-75.
5. Qi Jin, 2012. Detection and defence of Sinkhole attack in Wireless Sensor Network, Communication Technology ICCT, pp: 809-813.
6. Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques, 2012. International Journal of Distributed Sensor Networks.
7. Sheela, D., 2011. A non cryptographic method of sinkhole attack detection in wireless sensor networks, Recent Trends in information Technology, pp: 527-532.
8. Salehi, S.A., 2013. Detection of sinkhole attack in wireless sensor networks, Space Science and Communication (IconSpace), pp: 361-365.
9. Asha Nagesh, 2007. Distributed Network Forensics using JADE, IEEE transaction on Network security
10. Vokorokos, L., 2010. Host Based Intrusion Detection System, Intelligent Engineering Systems (INES), pp: 43-47.
11. Raghunath, B.R., 2008. Network intrusion detection system, Emerging Trends in Engineering and Technology, 2008. ICETET, '08: 1272-1277.
12. Macia´-Pe´rez, 2012. F Network Intrusion Detection System Embedded on a Smart Sensor, Industrial Electronics and IEEE Transactions on, 58(3): 722-732.
13. Haldar, N.A.H., 2012. An Activity Pattern Based Wireless Intrusion Detection System Information Technology, pp: 846-847.