IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

A Dynamic Analysis Model for Intrusion Detection in Mobile Network

Lavlish Goyal[1*], Nitika[2]

[1] Information Technology, ABV-Indian Institute of Information Technology, Gwalior, India
[2] Computer Science, PPIMT, Hisar, India

[*]*Corresponding Author: lgoel678@gmail.com, Tel.: +91-89494-51919*

DOI: https://doi.org/10.26438/ijcse/v7i4.511515 | Available online at: www.ijcseonline.org

Accepted: 14/Apr/2019, Published: 30/Apr/2019

***Abstract*— A** real time communication network having the open access features also suffers from various intruders. These intruders steal the communication information, disrupt the data or slow down the transmission. In this paper, a dynamic signature and parameter map based model is presented for intrusion detection. At earlier stage of this model, the log-event table map is performed to verify the authenticity of node. At this stage, the prevention from any external node is done under activity monitoring. In final stage, the communication observation under multiple parameters is done to identify the intrusion. The query pattern observation is applied in this stage to identify the attacked node and pattern. The proposed work model is simulated in NS2 environment with multiple query patterns. The observations show that the model has identified various attack patterns significantly.

Keywords— Signature, Query Pattern, Intrusion Detection, Activity Monitoring

I. INTRODUCTION

A real time network is having number of integrated communication criticalities. These criticalities are relative to network and domain nature. In these networks, the cooperative communication is applied without the inclusion of any centralized infrastructure. It means, the communication is performed with the help of other intermediate nodes. Each node needs to analyze the neighboring nodes so that the cooperative communication takes place. But as the inclusion of new nodes increases in the network, the network suffers from the threats of some communication attack over the network. These attacks can be at node level, layer level, communication level or the signal level. Each kind of attack is having its own criticalities and integrated restrictions. The attack formation and the association with communication constraints provide the ability to identify the attack category and the impact. Some of the common real time network attacks in dynamic cooperative networks are listed in table 1. The table has also presented the attack cause, impact and the associated constraints. The table includes the attack categorization which signifies that the attacks are an insider or outsider network attack.

Table 1: Network Attacks and Criticalities

Attack Name	Attack Type	Impact	Constraints
Black Hole Attack	Internal or External Node	Disrupt Data Forwarding	The infected node will accept the data packets and captures the communication from other nodes and disturb the actual communication
DOS Attack	Internal Node	Slow Down the communication	The node floods the heavy communication in surrounding nodes. The heavy communication occupies network bandwidth and the communication slow downs
Worm Hole Attack	Internal Nodes	Disrupt Packet Forwarding	Creates a communication tunnel between nodes pair so that the communication will not sent to destination.
Masquerade	External Nodes	Disguises the Node Identity and	Node is represented by separate identity of some valid node so that the communication will

		Signature	be revealed to that node.
Session Replay	External Node	False Identity of Node for Session	The unauthorized node is presented by some fake node so that the communication will be diverted to node.
Sequence Attack	Internal Nodes	Routing Attack as Sequence Changer	The node is applied on the network internal node so that the communication attack is applied in tracker.

To work with different attack forms, there are different detection and preventive methods elected by users. These approaches are effective to provide the communication improvement so that the safe and reliable communication will be formed. Some of the common categorization of these attack resistive methods is listed here under

A) Detection Methods

The attack detection approaches are generally defined specific to the attack type. The communication behaviour over the nodes is analysed respective to the attack so that the abnormal communication instance and participating nodes will be identified. Such as, the DDOS can be identified by observing the communication delay and transmission rate. In same way, black hole attack can be identified by analysing the communication throughput or the forwarding rate. These approaches can be applied in a group to identify the attack type at earlier stage based on the parameter specification later on the security constraints can be applied collectively to identify the attack criticality. The detection methods are also based on the layers and the application type. The relative rules or validations can be applied to identify the attack impact or the attack type so that the communication observations can be obtained.

B) Preventive Methods

The preventive method actually represents the attack independent methods applied to generate the effective communication route so that the safe routing will be performed. The preventive methods applied under various communication measures applied n all neighbour nodes and identify the safest communicating node as eligible next hop. The route formation over the good nodes can be considered as the effective network path so that the network route formation will be done. The routing is defined for optimizing the network QoS and network route formulation. The region specific analysis is applied for generation of effective communication node so that the reliable region effective node selection will be done.

C) Authentication Methods

The authentication is effective to verify the validity of a node. The network in which external nodes are involved, there is the requirement of node verification. The signature adaptive authentication method is required to provide the authenticity of nodes. Complete or the partial signature key map can be applied for proving the node level authentication. The cryptography methods can be integrated to apply the authenticity on nodes.

In this work, a dynamic parameter and signature map based model is presented for providing the reliable and safe communication in real time network. The work is defined in two main layers. In first layer, the signature verification is done to provide the node validity and later on the parameter based map can be applied for effective route formulation. In this section, different kind of attacks in real time networks are identified along with relative network challenges. The section has also explored the various methods for effective communication in the network. In section II, the work defined by earlier researchers is discussed. In section III, the proposed work model is defined and explored. In section IV, the results obtained from work are discussed. In section V, the conclusion from work is presented.

II. RELATED WORK

Attacks in the network are one of the most critical network challenges against the network security. The network suffers from various internal and external attacks. Different researcher proposed different preventive and detection based approaches. Author [1] provided a selective neighbour observation method for identification of attack nodes. Author observed the nodes behaviour under different parameters. These K-selected hops are analysed under communication loss parameters. Once the overhead node is identified, it is blocked as the attack node and provided a preventive route formation over the network. Author also generated the optimized communication route for safe data transmission. Author [2] provided a component specific multiple parameter based communication method for effective route formulation over the network. Author analysed the network under multiple parameters and observed them under the attack specific formulation. Author derive the communication method with preventive routing method. Author generated the exception driven route formulation over the network is drawn from the work. Author [3] provided a work on preventive route formulation in the network. Author provided the security context driven method for route formulation in the network. Author derived the node driven formulation so that the attack relative abnormality analysis and behaviour observation is done. Author provided the abnormality identification method for identification of misbehaving nodes. Author provided the communication over the normal nodes so that the safe and reliable communication will be formed over the network. Author generated the list of good nodes and provides the route by avoiding the safe communication over the network. Author

[4] has provided a hijacking attack detection and prevention over the network. Author provided the method for identification of spam node so that the effective node tracking will be done. Author provided the node spam tracking and communication and tracking so that the travel detection so that the reliable communication will be formed over the network.

Author [5] provided the identification of spam communication and generated a preventive communication measures over the network. Author provided the conventional technique for route formation and limit driven communication in the network. Author provided the threshold driven spamming so that the lifetime driven network route formation will be done. Author observed the neighbour nodes under cost parameter and generated the effective network nodes. Author [6] provided an improvement to existing OLSR protocol for intrusion detection. Author provided the identification of attack detection and prevention method so that the safe communication over the network will be formed. Author provided the work as the sink driven route formation along with blocked node identification method. Author identified the work as the improved routing measure so that the safe and reliable communication will be formed. Author provided a work on network feature driven measures to provide the safe communication measure. Author [7] provided the forwarding rule based communication measure for node level tracking so that the reliable route formation and rule formation will be done. Author identified the effective route and generated the effective route. Author [8] provided a work on real time network to analyse the communication distance under various parameters. Author divided the network in smaller zones and provided the communication by observing the nodes under different parameters. The work is applied to monitor the communication traffic for specific sessions so that the communication reliability will be improved. Author [9] has provided a work on behaviour driven methods for analysis on the network. Author provided the control flow driven route formation and network observation so that the reliable network tracking and the route formation will be done. Author provided the generation of safe node under multiple parameters. Author [10] generated the constraint map method with attack constraint specification. Author applied work on energy nodes in real time modelling so that the node level aspects will be analysed and the safe communication will be formed over the network. Author [11] provided the work on attack inclusive method for route formation under mathematical modelling. Author analysed multiple algorithms and provided a comparative derivation for route formation in the network.

III. RESEARCH METHODOLOGY

In this paper, an improved dynamic model is provided for intrusion detection in real time network. Author has provided the work in two main stages. In first stage, the map is applied to verify the node authenticity. Later on the attack detection method is defined for multiple parameters and for a specific communication session. In this stage, the node communication observation is applied dynamically so that the attack node and the safe nodes will be classified. As the attack nodes are identified, the nodes are set as the block node so that the exclusion in the participating list will be set. The communication nodes are also identified as the safe nodes which are considered as effective for the event communicating nodes. The model defined to generate the effective communication is shown in figure 1.

The figure signifies that the work model is divided in two main stages. In first stage, the first level estimation is done for signature map. The node level authentication is performed at this stage. The signature level map in the real time environment is performed for identification of the safe node. The signature map stage applied in this work is shown in figure 2.

During the signature map, the intermediate node is setup as the qualified server. The firewall server is setup so that the eligibility of node is done for effective communication over the network. Once the safe node list is generated, the next work is to analyse the neighbour nodes under different parameters. The parameters considered in this work are the communication loss analysis, throughput analysis and communication delay analysis.

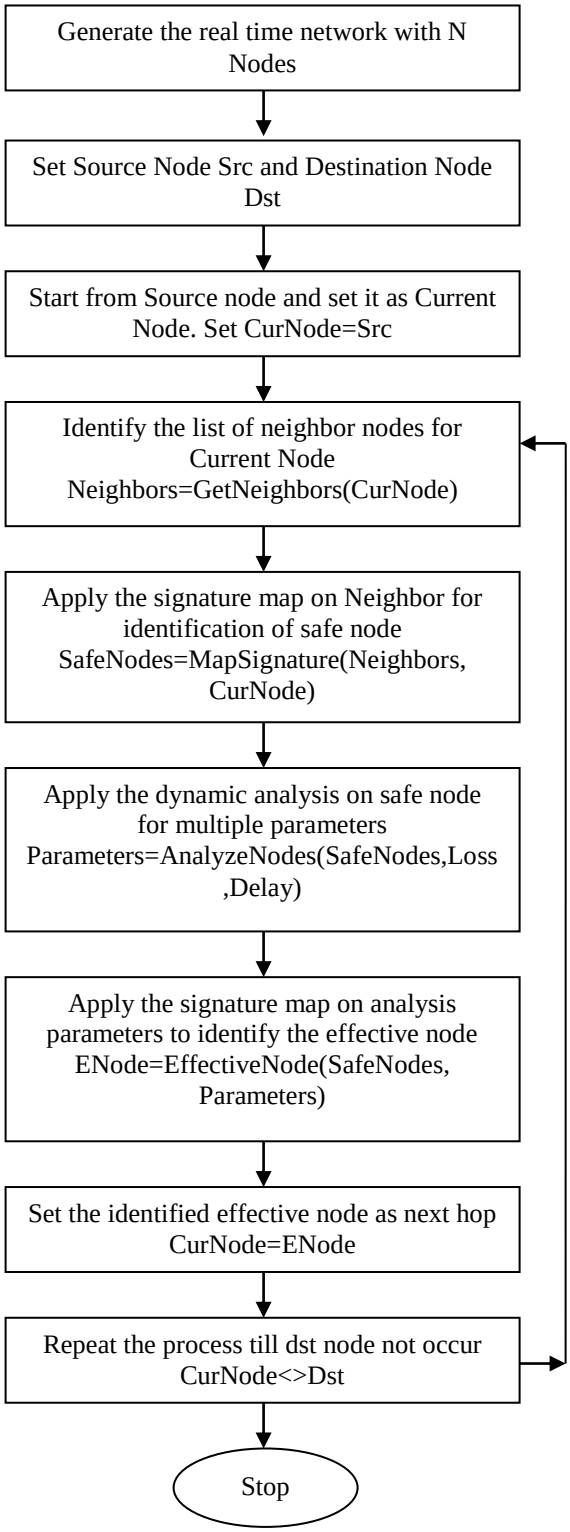

Figure 1: Proposed Method

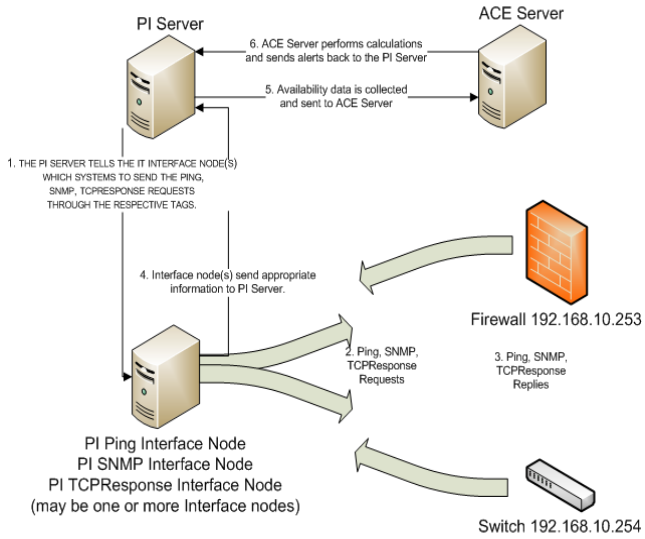

Figure 2: Signature Map in Real Time Network

The communication behavior analysis applied at the safe node. The node adaptability analysis so that the safe communication observation so that the communication criteria analysis will be done. At this stage, the identification of the node is node under loss and delay parameters. As a node with higher loss within the observation interval is identified, the node will be considered as the attack node and the particular node will be blocked. If the node is not a block node, the safe communication will be performed. The detection and prevention based combined method is provided to generate the safe communication route. The work is applied to achieve safe communication over the network.

IV. RESULT

The presented work is simulated in NS2 environment. The network node formations along with rule file specification. The rule file is having the query constraints so that the node level relaxation will be done. The communication structure observation along with rule formulation so that the effective rule effective analysis is done. The configuration elective analysis with rule map is applied along with acceptable communication nodes. The node functioning so that the log knowledge analysis so that the additional process communication so that the effective network formation will be done. Author provided the process model along with knowledge level observation and the elective node analysis is done. The query map based detection results is shown in figure 3.

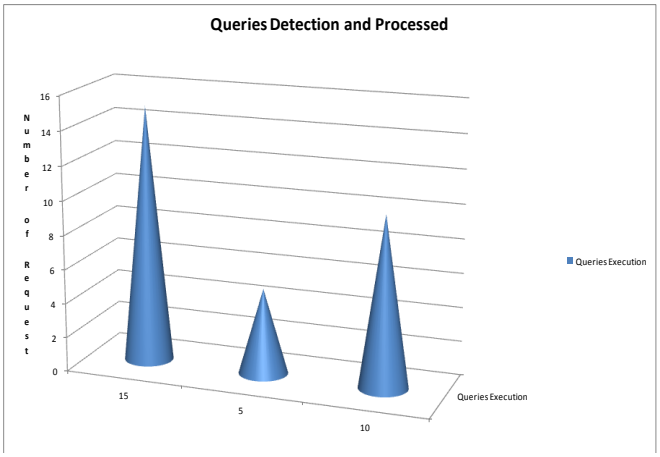

Figure 3 : Query Detection Results

Here figure 3 is showing the number of queries performed during the communication so that the effective communication will be formed. The query processed model is shown in this stage so that the effective communication will be performed. The intrusion detection modeling is showin in figure 4

```
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
168.160.128 -> 192.168.1.1
06/28-02:11:36.079578  [**] [1:10000002:1] INTRUSION DETECTED [**]
 {ICMP} 192.168.160.128 -> 192.168.1.10
06/28-02:11:37.080823  [**] [1:10000002:1] INTRUSION DETECTED [**]
 {ICMP} 192.168.160.128 -> 192.168.1.10
06/28-02:11:38.092668  [**] [1:10000002:1] INTRUSION DETECTED [**]
 {ICMP} 192.168.160.128 -> 192.168.1.10
06/28-02:11:39.100800  [**] [1:10000002:1] INTRUSION DETECTED [**]
 {ICMP} 192.168.160.128 -> 192.168.1.10
```

Figure 4 : Intrusion Detection Results

Here figure 4 is showing the intrusion detection against the proposed work model is shown here. The query map based signature analysis is applied. The figure showing the detected intrusion results.

V. CONCLUSION

In this work, an intrusion detection model based on signature map and the preventive and detection method is defined. At the earlier model, the work is here defined to generate the attack detection model. In first stage, the node level signature map is applied. Once the node authenticity is verified, the communication analysis is applied for loss analysis. The work is applied in NS2 environment under query map. The results show that the model has identified the node effectively.

REFERENCES

[1] Axel Krings," Neighborhood Monitoring in Ad Hoc Networks", CSIIRW '10, April 21-23, 2010, Oak Ridge, Tennessee, USA ACM 978-1-4503-0017-9

[2 Ying Li," Component-Based Track Inspection Using Machine-Vision Technology", ICMR'11, April 17-20, 2011, Trento, Italy ACM 978-1-4503-0336-1/11/04

[3] Bogdan Carbunar," JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks", WiSe'04, October 1, 2004, Philadelphia, Pennsylvania, USA. ACM 1-58113-925-X/04/0010

[4] Johann Schlamp," How to Prevent AS Hijacking Attacks", CoNEXT Student'12, December 10, 2012, Nice, France. ACM 978-1-4503-1779-5/12/12

[5] Joshua Goodman," Stopping Outgoing Spam", EC'04, May 17–20, 2004, New York, New York, USA. ACM 1-58113-711-0/04/0005

[6] Danny Dhillon," Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs", IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada. ACM 1-59593-306-9/06/0007

[7] Ahmed Khurshid," VeriFlow: Verifying Network-Wide Invariants in Real Time", HotSDN'12, August 13, 2012, Helsinki, Finland. ACM 978-1-4503-1477-0/12/08

[8] Evan Cooke," Toward Understanding Distributed Blackhole Placement", WORM'04, October 29, 2004, Washington, DC, USA. ACM 1-58113-970-5/04/0010

[9] Umair Sadiq," CRISP: Collusion–Resistant Incentive–Compatible Routing and Forwarding in Opportunistic Networks", MSWiM'12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10

[10] Mauro Conti," A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks", MobiHoc'07, September 9-14, 2007, Montréal, Québec, Canada. ACM 978-1-59593-684-4/07/0009

[11] Garima Gupta," Reference based approach to Mitigate Blackhole Attacks in Delay Tolerant Networks", Q2SWinet'12, October 24–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1619-4/12/10

Authors Profile

Mr. Lavlish Goyal pursued Master of Techanology from IIIT Gwalior, India in 2014. He is currently working in MNC as lead engineer in multimedia domain from 4.5 years.On his behaf,MNC has filled 8 patents in various countries including india and USA.

Ms Nitika pursued Bachelor of Techanology from JCD Sirsa and Master of Techanology from PPIMT hisar, India. She is currently teaching computer science to rural students.

