Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.632 – 637

RESEARCH ARTICLE

A Statistical Communication Analysis Model for Attack Detection in Mobile Network

Amit Kumar
Student, M.Tech
Deptt. Of Computer Sc. & App.
Pratap University, Jaipur

Omprakash Tailor
Student, M.Tech
Deptt. Of Computer Sc. & App.
Pratap University, Jaipur

Mr. Krishna Kumar
Assistant Professor
Deptt. Of Computer Sc. & App.
Pratap University, Jaipur

Abstract— **Security is one of the most critical issue of mobile network that ensures the reliable communication over the network. Because of dynamic property of Mobile Adhoc Network, the chances of the security issues increases. These attacks are incorporated at different security layers of the network. To handle these attacks, different researchers have defined many authentication based, prevention based and detection based approaches. In this paper, a description of one of such standard security model is presented based on the statistical analysis. The presented analysis model will perform the communication analysis under different attacks and analyze the severity of attack. The work is presented as the constraint based model description so that the reliable communication will be ensured.**

Keywords:* *Constraint Based, Statistical, Detection Machanism, Preventive Approach

I. INTRODUCTION

A mobile network is a dynamic communication adhoc network, in which any node can enter or exist to the network at any instance of time. Because of this, the external intruder node can easily participate in the network. The attacker node can also specify its identity that cannot be identify as a trustful node at the first time data access. Because of this, the criticality of the network is very high. All the layers of the communication network having the chances of attack infection. Each layer of communication network having different impact on the network, based on this impact and consequence analysis, different security mechanism are suggested[1][2]. These security mechanisms are divided in three main categories shown in figure 1.

The authentication approaches are basically used to identify the trustful nodes over the network. A node that proven its identity is considered as the trustful node. To perform this analysis, the safety rule is applied while performing the signature check of the communicating node. The authentication stage of the node is now improved with the involvement of different cryptographic approaches. These

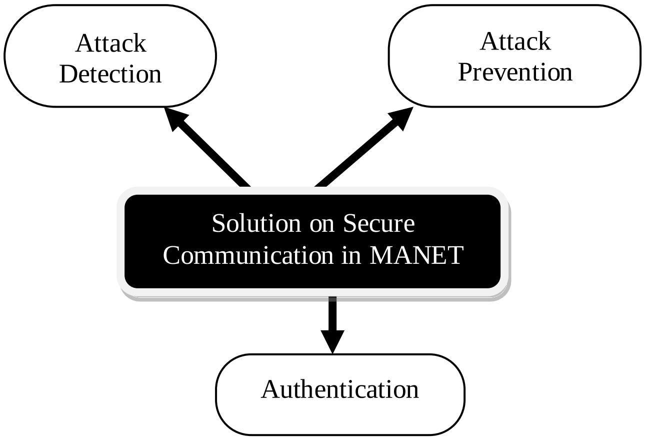

Figure 1 : Attack Solutions

cryptographic approaches include the public key cryptography, private key cryptography, image cryptography, visual cryptography, biometric cryptography and the DNA Cryptography. These cryptographic authentication schemes are either applied only once while proving the node identity or it can be applied with each communication[3][4].

Another secure mechanism to provide the attack safety is the prevention approach. In this approach, while performing the communication and detecting the next communicating hop, a safe node analysis is performed. The node that provides the most effective communication with higher throughput and the effective communication rate is considered as the valid safe node. In preventive approach, the communication is performed over these safe nodes so that more reliable and effective communication is drawn over the network[5][6].

The detection approaches are attack specific approaches in which, the attack based detection or the analysis is performed over the network. These detection approaches are either applied on individual nodes or the centralized node. Each attack having the separate node definition to detect the attack so that the effective network communication will be drawn over the network[7].

A Mobile Network is the most widely used communication network to provide different kind of data transmission. This network is available in public as well as in private domains. The network is having the dynamic nature, it means any new node can perform the communication participation to the network. Because of this the chances of the network security threats also increases. These attacks basically either destroy the communicating information or it reveals the information to the intruder. Some of the attacks and their relative impact on the network is listed in table 1. These attacks affects the different communicating layers of the network.

Table 1 : Security Attacks in MANET

Layer	Attacks	Solution
Application Layer	data corruption, Repudiation	Firewalls, dog watchers, antiviruses are installed to secure the application
Transport Layer	Flooding and Session Hijacking	Some kind of end to end security is implemented to prevent these attacks. Generally cryptography or secure authentication is implement to enable secure transmission
Network Layer	Routing Protocol Attacks such as DOS, Blackhole, wormhole	The attack detection or prevention algorithms are implemented along with specific protocol
Data Link Layer	Data Disruption, Traffic Monitoring	Provide security to MAC protocol with authentication based or hardware oriented security

Physical Layer	Jamming, Interceptions.	Use the hardware monitoring and avoid the jamming and denial of service and denial of sleep situations over the communication.

In this paper, a cooperative node analysis mechanism is defined to perform the attack detection in wireless network. In this section, the introduction to the MANET and the relative security aspects is defined. The section also defined the different attack handling approaches. In section II, the work related to the attack detection by the earlier researchers is explored. In section III, the algorithmic approach adapted in this work for attack detection is explored. In section IV, the conclusion obtained from the work is defined.

II. LITERATURE REVIEW

Lot of work is already done in the area of attack detection and prevention. Some of the work done by the earlier authors in the same area is discussed here under.

Axel Kring has defined a work on neighbor node monitoring to identify the misbehaving nodes. Author defined k-hop analysis approach identify the bad or the malicious nodes. Author has exposed the associated overhead of the attack detection. Author defined the misrouting analysis approach over the Mobile Network[1]. Author work on network node component detection under the video transmission analysis. Author defined the probabilistic analysis based mathematical modeling approach for the attack detection. Author also defined the work under different exceptions so that the effective communication will be drawn from the communication [2]. Another work on the malicious node preventive routing in hybrid network was defined by Bogdan Carbanar. Author defined the work under the security aspects in context of the cellular node analysis. Author defined the study on different attacks and the abnormality behaviors and perform the identification of well behaved nodes over the network[3].

Another work on Hijacking attack prevention was defined by Johann Schlamp. Author defined the study on the attack and to detect the spamming over the network. Author defined IP prefix based hijacking so that maximum benefits will be derived from the communication. Author analyzed the current as well as long term benefits to provide the reliable communication[4]. Another work on the spam detection and prevention in such network was proposed by Joshua Goodman. Author defined the conventional technique by applying the thresholding to the spam limit. Author imposes the message cost and identify the spamming effect over the lifetime analysis so that the effective cost challenges will be handled[5]. A work on the IDS detection under the OLSR protocol was defined by Danny Dhillon in year 2006. Author defined the work to reduce the false positive and false negative reduction. Author presented the work on link state routing protocol to improve the communication over the network[6]. Another work on network invariant analysis was proposed by Ahmed Khurshid in year 2012. Author defined the software level analysis over the network and performs the intrusion detection under the forwarding rule. The node communication analysis with least forwarding will be tracked as the attack position over the network[7]. A work on the blackhole node detection in distributed Mobile Network was defined by the author. Author has performed the difference analysis over the network node blocks under the traffic monitoring and perform the analysis over the attack. The effective node detection is performed to identify the effective node communication so that the communication reliability is obtained[8]. A work on collusion resistant incentive routing on the forwarding node analysis was defined by Umair Sadiq. Author defined the work on opportunistic network to perform the analysis on optimal node behavior and to control the network flow so that the reliable communication will be performed over the network[9].

Another work on randomized, effective and distributed protocol based work was presented by Mauro Conti. Author performed the work against the replication attack in sensor network. Author defined the work on constraint analysis in the sensor network environment. Author defined the adversary model to improve the security over the network[10].

Grima Gupta has defined a referenced analysis on the mitigation of blackhole attack in Mobile Network. Author presented work on the routing algorithms to improve the network effectiveness. The work was the combination of forwarding communication information along with probabilistic analysis. Author defined the work on DSG based analysis to perform the attack detection and mitigation[11]. A work on topology based security was presented by Abhijit in year 2011. Author identify the security threats and reduce the detection rate.

III. PROPOSED WORK

In this paper, an effective approach of attack detection and prevention is defined based on the cooperative node analysis. The cooperative node analysis is here defined as the set of neighboring nodes that performing the regular communication with the current node. The analysis is here defined under multiple parameters. The communication parameters for the analysis is defined here in figure 2.

The user information based host node analysis is defined under different attacks and the problems. At the initial stage, the identification of the cooperative nodes is done by performing the history based communication analysis. As these nodes are identified, the next work is top perform the analysis on these cooperative nodes to identify the most effective next hop selection.

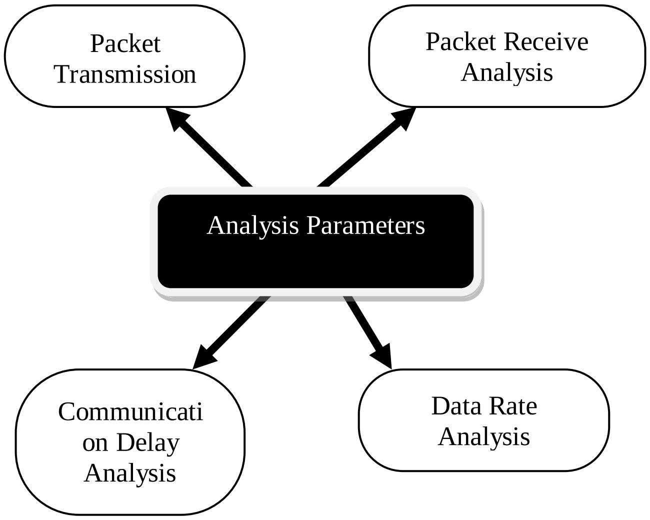

Figure 2 : Communication Parameters

The host node analysis is done to perform the safe node identification over which the communication will be performed.
The analysis mechanism adapted in this present work is listed here under
The node analysis is here defined under the statistical decision shown in figure 3.

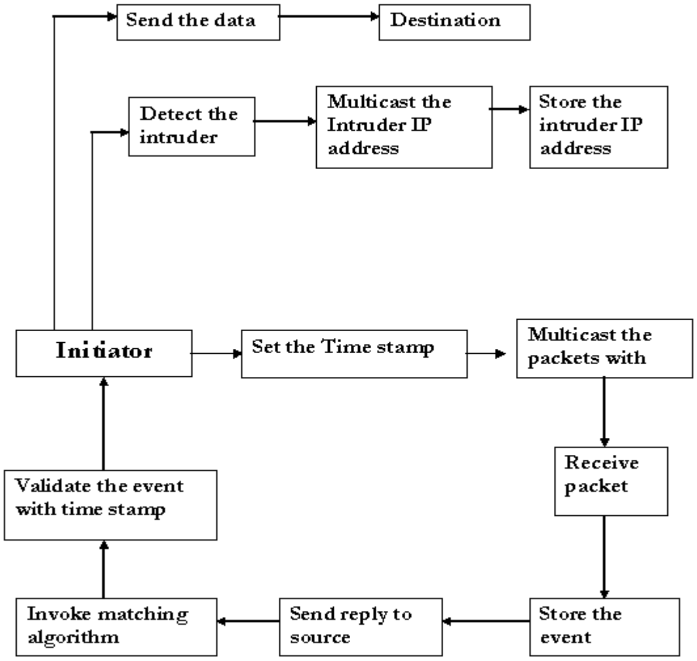
Send the data
Destination
Detect the intruder
Multicast the Intruder IP address
Store the intruder IP address
Initiator
Set the Time stamp
Multicast the packets with
Receive packet
Validate the event with time stamp
Invoke matching algorithm
Send reply to source
Store the event

Figure 4 : Analysis Sequence

The main steps of this analysis system is described here under

1. The traffic monitoring over the system is performed
2. The outgoing traffic monitoring is performed
3. Source oriented packet monitoring is performed
4. The monitoring of the packets coming from the outer source is done.
5. The communicating packets to the next hop is also performed
6. The incoming packet analysis is performed.
7. The communication between any node pair is also analyzed.
8. The sink oriented packet analysis is performed.

Once the cooperative communication information is retrieved, the next work is to perform the statistical analysis over this node to identify the communication association between nodes. These nodes are analyzed respective to the current node analysis. This association vector is used to identify the actual communication parameter as the cost vector. This cost vector work as the decision factor for the selection of next hop.

In the same way, the next hop selection is done and in same way the complete communication path is constructed. The route construction is presented as the effective safe path over which the communication will be performed.

The presented work will be capable to provide the effective communication over the network.

IV. CONCLUSION

In this paper, an effective cooperative node analysis approach is defined to provide the effective communication in Mobile Network. This work includes the cooperative node analysis under the multiple parameters. Based on this analysis the node cost will be identified. The nod with least cost will be selected as the next reliable hop. The routing path based on this communicating hop is constructed.

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