International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 07, July 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

An Agent Based Approach for Sinkhole Preventive Route formation in Mobile Network

Rekha[1], Radhika Garg[2]

[1]Research Scholar, M.Tech, [2]Assistant Professor, Deptt. Of Computer Sc. & Engineering, Vaish College of Engineering, Rohtak, Haryana

ABSTRACT

The open and public availability of Mobile network suffers from different kind of internal and external attacks. Sinkhole is one such critical attack in which the network node generates a fake identity of sink node and captures the network communication. In this paper, an agent based communication evaluation method is defined to identify the sinkhole node and to generate the safe communication over the network. The work is defined to define the dynamic selection of events over the network based on the coverage and connectivity analysis. Later on, the agent performed the evaluation on neighbor nodes based on communication loss, communication delay and packet communication parameters. The proposed work is implemented in NS3 environment. The simulation results show that the method has improved the packet delivery ratio and reduced the communication delay and communication loss.

Keywords: Mobile Network, Sinkhole, Communication Analysis, Coverage Analysis, Security.

II. INTRODUCTION

Mobile network is the dynamic network form in which network nodes are available in the open environment. The infrastructure less network provides the cooperative communication between the network nodes. Different forms of voice and data can be communicated in the form of calls, SMS and message communication. But this open network also suffers from different kind of security threats at node level and network level. Various internal and external attacks affect the network reliability and the network suffers from different kind of attacks. These attacks include blackhole attack, wormhole attack, and sinkhole attack. Sinkhole is the attack that can occur by any internal or external node by generating the fake identity. Any network nodes which have network access represent itself as the sink node of the network. The sinknode accepts the packet communication to the actual destination node and not forward it to the sink node. Because of this, the network suffers from heavy communication loss. The existence and the behavior of sinkhole attack is shown in figure 1.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 07, July 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

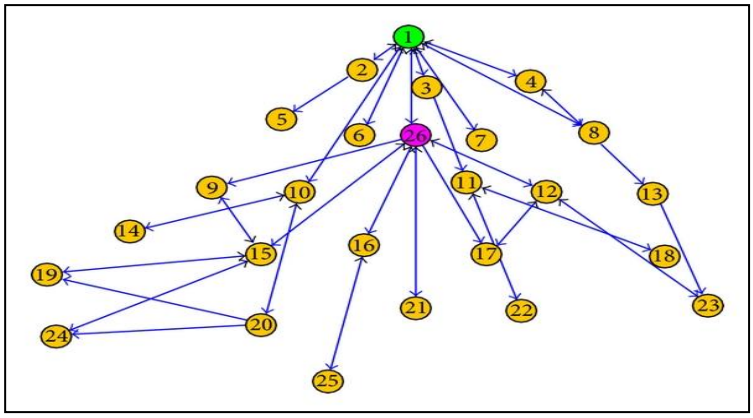

Figure 1:Existance and Behavior of Sinkhole Attack

Sinkhole is generated as the fake identity so it is considered as the authentication based attack. The node level trust evaluation is required to generate the safe communication in the network. The trust can be based on the control message tracking, generation of authentication bits or by setting up some cryptography method. Another way to secure the communication against sinkhole attack is the preventive algorithm specification. It means to generate the communication path by avoiding the sinkhole nodes. The preventive route can be formed to generate and safe and reliable communication. The sinkhole attack can destroy the communicating information and allow the intruder to capture the information. The sink hole attack can work on different network layers including the application layer, network layer, data link layer and transport layer. In this work, a preventive method is defined to generate the safe communication against sinkhole attack.

In this paper, an agent based analysis method is defined to generate the safe communication over the mobile network in existence of sinkhole attack. The communication parameter based evaluation is provided to generation of preventive path. In this section, the basic behavior of sinkhole attack is discussed. The paper has defined the effect and solution of sinkhole attack. In section II, the work defined by the earlier researchers is discussed. In section III, the research methodology is defined for generation of agent based route formation method against sinkhole attack. In section IV, the comparative analysis results obtained from the work are provided. In section V, the conclusion obtained from the work is presented.

III. LITERATURE REVIEW

The sinkhole attack is the crucial attack occurs in mobile network by generating the fake identity of sink node. The work provided by the researchers to detect the sinkhole attack is discussed in this section. Author[1] has defined a work on neighbor level monitoring to identity the misbehaving nodes in the network. The association specific analysis was performed in this work to identify the attacker or misbehaving node. The probabilistic measure is applied to perform the evaluation at node level and to detect the sinkhole node. Once the attacker is identified, the safe route formation is done. Author[2] has defined a work to optimize the network communication based on the mathematical evaluation. The communication statistics was analyzed by the author and generate the preventive route. The malicious node detection is provided by the author to achieve the secure communication. Author[3] has provided a study on different sink hole in the network and to identify the misbehavior of network nodes. The detection of the attacker node was done along with generation of safe route with abnormality evaluation. The attack specific route formation was provided to generate the safe path in the

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

network. Another work on sinkhole attack to identify the spam communication was provided by the author[4]. The network layer based tracking was provided to analyze the communication sequence and the bad packets. The long term observation on the communication pattern was considered by the author identity the misbehavior of the network nodes. The identification of the safe and unsafe nodes is done by the author and based on it the safe communication was identified by the author. The preventive route formation is provided by the author to improve the communication reliability. Author[5] has used the preventive route formation using conventional mapping technique. The threshold limit on the communication frequency is applied to observe the behavior and the cost. Once the cost is evaluated, the route formation based on the analysis is done. Author[6] has defined a protocol adaptive work to observe the invariant communication analysis. The intrusion detection was applied by the author under the forwarding rule. The node level tracking and the hole identification was defined by the author to improve the communication failure and to recognize the false data communication over the network. Author[7] has defined the software level processing to detect the intrusion over the network. The forwarding rule is defined at node level and network level to detect the intrusion over the network. The node level tracking under the forwarding node evaluation to identify the safe routing in the network. The sink hole is the position node in the network that captures the network communication and the communication loss occur in the network. Author[8] has provided a work on the distributed mobile network and to generate the safe communication. The traffic level observation and the node tracking was provided to achieve the traffic monitoring. The sink hole analysis is done based on the incentive evaluation at node level. Author[9] has used the node detection method and collusion resistant incentive routing for the opportunistic routing. The node behavior was analyzed in a controlled manner to identify the safe and unsafe nodes over the network. Once the attacker node is identified, the reliable communication is performed over the network. The node level optimization in the distributed network is performed. The node level mitigation was provided for improving the network communication. Author[10] has applied the constraint driven analysis on the sensor nodes to generate the safe communication route against the sinkhole attack. The security driven improvement was achieved by the author. The node level evaluation was provided to generate the safe communication in the network. Author[11] has defined a probabilistic and mathematical model to analyze the communication behavior of node. Based on this the sinkhole detection and prevention based route formation was provided. Author[12] has used the security driven analysis to the mobile network. The threat drive observation on different communication parameter was provided by the author and later on applied the evaluation at node level to generate the safe communication path. The method has reduced the loss rate and improve the network effectiveness.

IV. RESEARCH METHODOLOGY

In this present work, an adaptive work model is presented to improve the communication against the sinkhole attack. The sinkhole attack modify the actual routing information and increase the communication loss by setting the fake destination nodes. In this work, an agent based route observation method is defined to avoid the inclusion of fake destination nodes. The proposed communication model is shown below

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

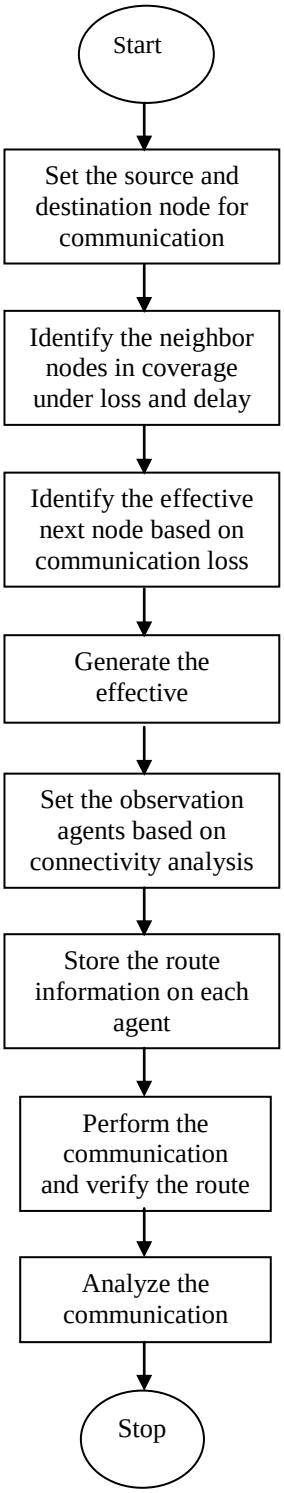

Figure 3.1 : Flow of Work

Fig. 3.1 is showing the flow of work related to represent the proposed work. In this work, the network is defined with randomly distributed mobile nodes. The network is defined with specification of source and destination. The algorithmic process starts from the source node and moves to the destination node by performing the node specific analysis. The coverage based observation on the intermediate nodes is applied to identify next effective node. The connectivity analysis and the route formation is done so that the communication to the next immediate node is performed. At the end, the analysis of the communication is performed.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 07, July 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

V. RESULTS

In this present work, a preventive route formation method is defined against the sinkhole attack. The proposed approach is based on the agent establishment on the network and to perform the agent based network analysis. The communication statistics over the session is analyzed to identify the safe and unsafe nodes. Once the unsafe nodes identified, the preventive route is framed. The proposed approach is simulated on a random topology based mobile network in NS3 environment. The comparative results are generated in terms of communication throughput and communication loss.

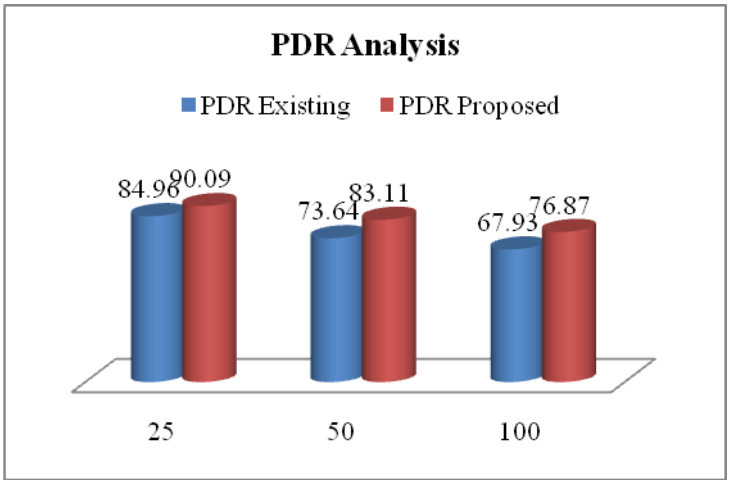

Figure 3 : PDR Analysis

Here in figure 3, the PDR based analysis is applied on the existing and proposes approaches. The packet delivery ratio represents the successful communication performed over the network. The results show that the proposed method has improved the communication delivery in the network. Another important parameter considered here is communication loss. The communication loss is about to analyze the data drop during the communication. The evaluation of the proposed work in terms of communication loss is shown in figure 4.

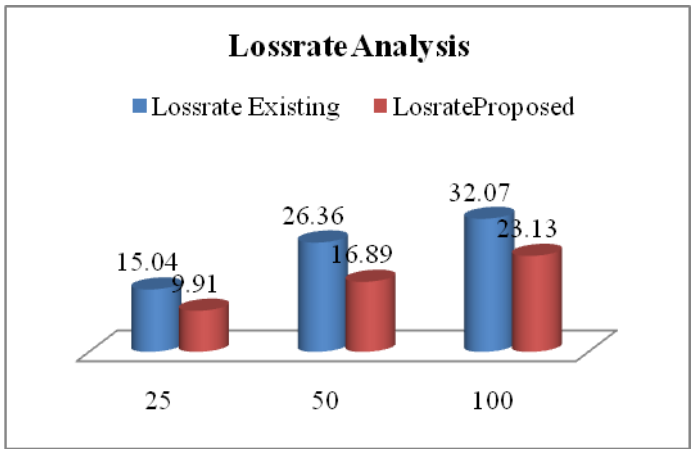

Figure 4: Lossrate Analysis

Here in figure 4, the Lossrate based analysis is applied on the existing and proposes approaches. The lossrate represents the communication drop occur during the communication in the network. The results show that the proposed method has improved the communication delivery in the network and reduced the communication loss. The results shows that the proposed model has improved the network communication and reduced the communication loss.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

VI. CONCLUSION

The mobile network suffers from different kind of network attacks. One of such attack is sinkhole attack in which the node creates the fake identity and diverts the network communication. In this paper, an agent based approach is defined to optimize the network communication. The agents have analyzed the coverage area and identified the safe and unsafe nodes. Based on the observation, the safe communication is performed in the network. The simulation results shows that the proposed model has improved the packet delivery ratio and reduced the communication loss in the network.

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 Sink Holes", 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 Sink Holes 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 Sink Holes in Delay Tolerant Networks", Q2SWinet’12, October 24–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1619-4/12/10