International Journal of Advanced Computer Technology (IJACT)
ISSN: 2319-7900 Volume VIII, Issue III, June, 2019

A Novel IDS Security Scheme for Multicast Communication in DTN

Shivali Pandey, Prof. Anshul Sarawagi, Department of CSE, I.E.S. Collage of Technology, Bhopal, India
Shivalipandey26@gmail.com, Anshulsarawagi301@gmail.com

Abstract**—***This DTN routing should naturally support unicast and multicast routing strategies. A network node can register itself to any receiver group by setting the corresponding destination. In this research we proposed a new security algorithm with multi cast routing against malicious packet dropping attack in DTN. The proposed security method of finding attacker is based on the link detection method for data forwarding in between sender to receiver. The packet dropping on link through node is detected and prevented by IDS security system. This method not only identified the black hole and grey hole but also prevent from routing misbehavior of malicious nodes. The attacker is identified by data dropping of packets in excessive quantity and their prevention is possible by selecting the next possible route where attacker does not exist in connected link between senders to receivers. The intermediate nodes are identified the attacker through confirm positive reply of malicious node or nodes in dynamic network. The proposed secure IDS (Intrusion Detection and prevention) is securing the DTN and improves the network performance after blocking black hole and grey hole in network. The network performance in presence of attack and secure IDS is measures through performance metrics like throughput, routing packets flooding and proposed secures routing is improves data receiving and minimizes dropping data network.*

Keywords:- Malicious Attacker, routing, Security, DTN, IDS, Nodes.

I. INTRODUCTION

Delay Tolerant network in [1] that they provide specification and an application interface to synchronize forwarding of messages among a partition based mostly network in which topology changes endlessly and provides long delays. it's an infrastructure less wireless network. It conjointly experiences frequent and better length partitions because of nodes in DTN are intermittently connected and sending data to single as well as multiple nodes [2]. DTN network provides no guarantee that a path from source to destination can stay same at on every occasion instance by that are able to end that two nodes will ne'er exist in a one connected portion of the network. A number of routing techniques based on first for probabilistic behavior of nodes in contact second one for social behavior of nodes in contact and third for context and content awareness for communication [3] have been proposed for DTN. All of these routing techniques evaluate nodes in contact to find the potential forwarder to the destined node for messages stored in their buffer space. One challenge of DTNs is the intermittent connectivity while another challenge may be the handling malicious or selfish attackers who may inject bogus messages in the network. In DTNs, the messages can be sent over an existing link and buffered at next hop. Whenever, the next hop comes in range, the message is transferred to that node. This message propagation is called as "store carry forward" i.e. when a node receives some packets and it stores these packets into its buffer, carries them around it until it contacts another node and then forwards the packets. In DTN, the routing is decided in an opportunistic way [4]. In routing Flooding strategy and Forwarding strategy [5, 6]. Flooding strategy is based on the principal of replicating messages to enough nodes so that destination nodes must receive it. Forwarding strategy uses knowledge about network to select best path to the destination.

II. DIFFERENT TYPE ATTACK

Attackers nodes are performing different types of malicious activities that have damage basic aspects of security like integrity, confidentiality and privacy [7]. Here there are different types of attacks [8, 9] and their mentioned in detail.

A. Active Attacks

It is like as passive attack that monitors and listens by unauthorized communication channel and it also modifies data stream in communication channel. These attackers are actively participating in network in malicious performance. There are different types of active attacks a shown here.

1) Blackhole Attack

Blackhole attack is the packet consumption attack. In this attack the attacker nodes is identified the sender that want to send data to receiver and reply fake route information to sender. Sender is sending the data from the path where the attacker is existing in network. Then in that case the attacker is loss whole data and network performance is degrading.

2) Sybil Attack

Malicious node can duplicate itself and its presence affects at multiple places. It targets fault tolerance scheme as distributed storage, multipath identities for another node, multipath routing and topology in the networks. These attackers are changing their original identity and grasp the neighbour node identity in network.

3) HELLO Flood Attack

An attacker with high radio transmission range and process on power sends “HELLO” packets to number of mobile nodes which are isolated in wireless mobile network. So mobile nodes prejudice adversary is their neighbour. While information is sent to the base station, then at that time, the victim nodes are trying to go via attacker resulting neighbour in higher spoofed.

4) Denial of Service

When unintentional failure of nodes or malicious nodes attack any event that diminishes network’s capability of services and also affect on destroying network, this can be affected on different layers like Physical layer and DoS attacker in jamming and tampering. While collision, unfairness and exhaustion will occur in Link Layer confirm the presence of DoS attack.

5) Wormhole attack

Wormhole attack is most severe attack in DTN in which using private high-speed networking, pair of colluding attackers can record packet information at one location and replay then on other location. So, this can be launched against all communications for providing authenticity and confidentiality.

B. Passive Attacks

It does not affect any communication works but unauthorized person can just monitor and listen communication channel and it is hard to find these types of attacks due to its passiveness behaviour. The passive attackers are not continuously and actively injecting malicious actions in network because of that their reorganization is difficult.

1) Attacks against privacy

In mobile network there are large numbers of information available by remote access, so any malicious node can easily gather information. Here some attacks against privacy are defined:

2) Monitor and Eavesdropping

It is very common attack, in which, by snooping data adversary it can easily discover communication control information for mobile Ad hoc network configuration that contains information and affects against privacy protection.

3) Traffic Analysis

Though messages are transferred by encrypted, it leaves high possibility communication patterns, because of mobile activities and it can potentially affect on enable information and cause harm to mobile network.

III. LITERATURE SURVEY

The In this section we actually discuss the work in the field of security proposed by different researchers. Many researches are interested to provide security in network.

In this [20] proposed the system is deliberatively designed to under standard networking norms to fulfill the networking protocols and standard, this improves the proposed Statistical-based Detection for GrayHole and BlackHole attackers (SbDGB) technique to be appended on universal nodes. The initialization of system is done with configuration settings and node alignment with respect to the networking standards and infrastructural design protocols to meet the research agenda on universal platform. previous techniques increase the load overhead of the system and thus in SbDGB technique, a series of typical approaches are interchanged as justification and detection is primarily conducted followed by confirmation and verification to make the system swift in detection.

In this paper [21] has been proposed a title "Quota-Based Multicast Routing in Delay-Tolerant Networks" they propose quota-based multicast routing approach they can not only achieve a high delivery rate but also adapt to network conditions. Most importantly, their proposed approach need not maintain group membership. In other words, any concerned members can freely join and leave any multicast groups if they will in radio range, and this feature suitably fits into Delay tolerant environments. That work further enhanced by extra overhead minimization based that is like latency minimization, data error rate minimization etc.

In this paper[22], work in the field DTN security and proposed a title "Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks" in this paper they provide a security analysis of the current DTN RFCs and proposed security related internet drafts with a focus on space-based communication networks, which is a rather restricted subset of DTN networks. They focus the bundle security while group communication involves, further each layer security is inbuilt from given work and increases the privacy and reliability of the DTN communication.

In this paper [23] has a title "A price-based interactive data queue management approach for delay-tolerant mobile sensor networks" This paper presents a price-based interactive data queue management approach (PI-DQM) for delay-tolerant mobile sensor networks (DT -MSN s) to address the priority deviation problem during the data transmission process. The method is transparent to prioritized data packets. That work further enhanced by applying priority mechanism into the TCP, UDP data packet for separation of acknowledgement and acknowledges lees service in MANET and it also identifies the unwanted data by priority identification of data packets.

IV. PROPOSED MODEL FOR IDS

The IDS provide the actual value to each node. The X and Y value is exactly equal to the selected hop count value. The route is actually selected on the basis of minimum hop count and the two variable X and Y compare hop value at the time of data sending by sender in network.

This research center point is how performance of network will affect under routing misbehavior attack in a network and how the proposed IDS block the malicious activities of attacker and provides secure routing after proving the valid variables value.

$$X_{VALUE}=Y_{VALUE}\text{.........................eq.(1),}\quad X \leq y$$

Value =1 means one sender and one receiver sender and so on. It implies that the difference in these two-path variable is equal to zero. That means the hop count value on each node is measure.

$$X_{VALUE}-Y_{VALUE}= 0\ \text{............................eq. (2)}$$

The path between the nodes is not identified correctly but, in this research, verifies the path i.e. selected by attacker for dropping the data packets.It actually measur3s the value of hop count. The proposed method will improve network routing performance measure through performance metrics like throughput, packet dropping and routing load in presence of attacker and after applying proposed security scheme. In this section first we mentioned consider assumption of network is as follows:-

Number of nodes (Nm) = 40 // Total number of nodes including IDS and Attacker

Consider Routing Protocol = ODMRP

Malicious attacker behavior = (Packets Dropping)// MA

Security Provider = IDS (Intrusion Detection System) // Security Procedure

Nodes Radio Range (RR) = 250m // in meters unit

Steps of Algorithm

Step1: *As we know that the for proper communication in DTN sender first sending the Route Request(RREQ) to all nearby nodes that are directly in radio range of senders (ST). The intermediate nodes may be equal to one or more than one.*

T=1, 2, 3...... // depend on number of senders.

Step2: *In dynamic network most of the time is possible destination is not directly available. The intermediate nodes forward the request of sender till destination not found. The current record of route is maintained up to destination. .*

T=1, 2, 3.......// depend on number of destinations

// The Quantity of Sender and Receiver is always equal //

Step 3: *If the sender is confirming the route to Destination (DT) then select the route of shortest hop count and deliver data through that minimum path length (XVALUE) and also one variable YVALUE stores XVALUE value for confirming multicast data delivery up to destination.*

Data packets containing the value of hpp count or path length and each hop count increment XVALUE reaches to YVALUE.

∑XVALUE = (X1, X2, X3…….Xn) up to destination is Minimum then select it for data sending with holding the value of (YVALUE) and also next route of hop count X1, X2, X3 …….Xn≥ Min path length then identified the possibility of attacker.

The X1, X2, X3 …….Xn≥ Min path length is decided by secure IDS in presence of attacker.

Step4: *For identified the Black hole and grayhole malicious behavior IDS system is to calculate path length through Xn=XVALUE and Yn=YVALUE, if these variable difference is zero matched (eq. 2). It means no attack in the network; path is secure, and data packets forwarding is proper in between Ss to Dd.*

Step 5: *The secure IDS (Intrusion Detection system) verify if routing information of hop count selected by attackers is not matched related to actual routing information of hop count length, that confirm some routing misbehavior activity occurs in the network through malicious nodes.*

Step 6: *If the hop count calculation provides some negative values, and XVALUE, YVALUE (eq. 2) conditions are not matched. That confirms the attacker presence MA(M Attacker node)*

If path length or hop count = {X1, X2, X3...........Xn ≠ Yn} for D1,2,3....i in single path.

Step 7: *If the step 6 condition is true that shows no data is delivering through that path, insert new entry in routing table which contains path information to destination. Otherwise go to step 2*

Step 8: *If next hop count value is countable and XVALUE is not incrementing as equal to YVALUE that means this link is not reliable for communication. If data forwarding information is false then send the data packets by checking the reliability through get the true value if data is received at destination.*

Step 9: *The secure IDS prevention scheme blocks that node i.e. attached to that path and changes the actual path of sender for sending data. Also forward the nodes identification in network by that the attacker will never select in routing procedure by any sender.*

Step 10: *If the attacker is present in selected path for data delivery then avoids that path and preferred another suitable paths established by MAODV.*

Step 11: *Attacker exist path length X1, X2, X3 …….Xn=Min then // selects attacker free path*

Step 12: Select route of path length X1, X2, X3 …….Xn≥ Min // avoids shortest path

Step 13: *Then forward data packet until send all data packet reach to destination so no attacker is present in network.*

Step 14: *If bundles of data packets forwarding and route information is correct then it is valid condition of routing in network and go to step 2.*

Step 15: *Exit*

The example of proposed security system with its working is mentioned below in presence of attacker. The proposed scheme works to count whole length of path from source to destination.

V. SIMULATION RESULTS

The simulation results are showing the performance of SbDGB, Attack and proposed BIPS multicast routing in DTN network. The proposed multicast protocol are improves sending and receiving by maintaining proper channel information.

A. PDR Performance Analysis

Multicasting is intended for group-oriented computing. There are more and more applications where one-to-many or many-to-many dissemination is an essential task. Each node along the route, when transmitting the packet to the next hop, is responsible for detecting if its link to the next hop has broken. In DTN network the delay is overcome i.e. mainly occur due to mobility of mobile nodes. In this graph the PDR performance of proposed BIPS MAODV protocol for DTN network is enhanced and provides higher packets percentage about 95% successful data receiving but in case of SbDGB it is 80% and Attack is only 52%.

B. Routing Load Analysis

When a source node needs to send a packet to a destination node for which it has no routing information in its table, the Path Discovery process is initiated. In the request phase of sender, a node explores the environment. Once the request reaches to the destination through intermediate nodes the response phase is entered and establishes the path. The number of routing packets in DTN network in proposed BIPS MAODV protocol is about 2000 up to end of simulation but in case of Attack and SdDGB it is much higher i.e. about 4000 and 2900 in network. The main reason of enhanced routing overhead is not proper handling the mobility of nodes in network.

C. Throughput Performance Analysis

In mobile network contains each and every node is called a multicast router, which are logically connected to each other directly or indirectly. These mobile routers manage group membership and cooperate to route data to all hosts wishing to participate in a multicast group. The proposed protocol group communication is based on specific bundle-based communication between the sender and receiver. The throughput performance of proposed BIPS MAODV is much better in DTN network. Here the throughput is about 190 packs/seconds maximum and 120 minimum rest of the performance of Attack and SbDGB is very low.

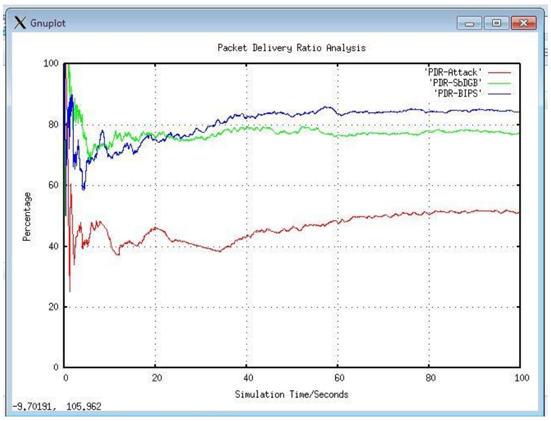

Fig.1 PDR Analysis

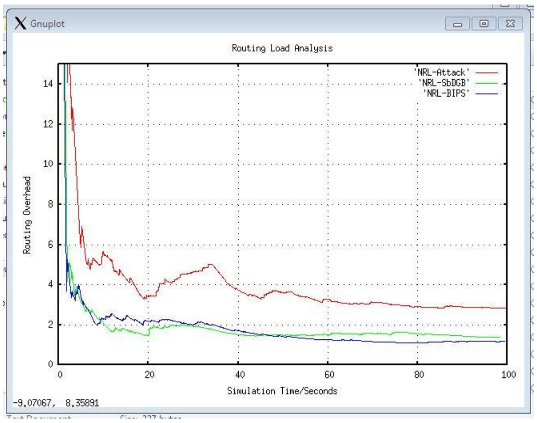

Fig.2 Routing Packets Overhead Analysis

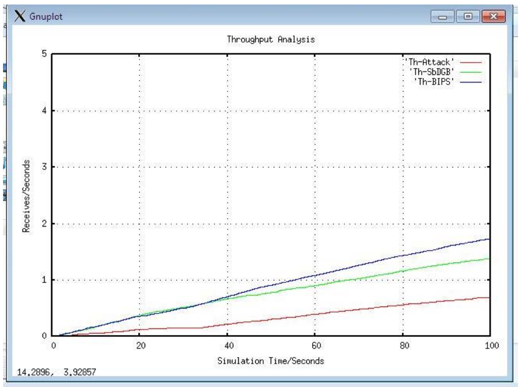

Fig.3 Throughput Analysis

D. Delay Analysis

The Delay Analysis specifies the how long it takes for a packet to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes. Delay cannot be null because to travel a distance each packet requires SME time. The Delay Analysis performance of proposed BIPS MAODV is much better in DTN network. Here the delay is very minimal in case of BIPS as compared to that of Attack and SbDGB

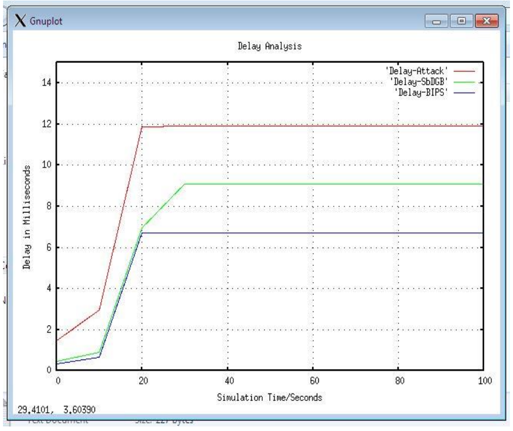

Fig.4 Delay Analysis

VI. CONCLUSION AND FUTURE WORK

The nodes in dynamic network are mobile and forming a temporary connection in between sender and receiver through intermediate nodes or sometime directly. The multi cast routing protocol is transferring the data in between sender and receiver through intermediate nodes. The connection establishment up to destination through source having a combination of normal nodes and malicious node and attacker aim is to drop data packets sending by sender to destination after connection establishment. Black hole and Grey hole always tried to be a part of fake path established by attacker for loss data packets. In this research the proposed reliable and novel IDS (Intrusion Detection System) is identified the attacker/s routing malicious activities of packet dropping. This malicious actions of attackers are degrading the routing performance of network. After detecting Black hole and Grey hole the proposed secure mechanism is also prevent from attacker by deny the possibility of routing through malicious nodes. The performance metrics shows the difference in performance of attacker and proposed IDS and clearly conclude that performance of proposed scheme is proving the secure communication. The PDF is about 97% and in presence of attacker is very poor, about less than .5%. The packet dropping is reduced and enhance receiving of data packets. The performance of transport layer protocol is also satisfactory.

In future also the simulation is performing through different routing protocol like OLSR and multipath routing protocols. Apply the same detection and prevention scheme to secure routing protocol. The network is dynamic that's why also applying Location Tracker System to trace attacker easily and also aware forwarding massage to nearby nodes of network about malicious activities and apply proper Location based security scheme.

REFERENCES

[1] A. Lindgren, A. Doria, and O. Schelen, “Probabilistic routing in intermittently connected networks,” SIGMOBILE Mobile Computing and Communications Review, vol. 7, 2003.

[2] Wenrui Zhao, Mostafa Arnrnar and Ellen Zegura, "Multicasting in Delay Tolerant Networks: Semantic Models and Routing Algorithms," in Proceeding of SIGCOMM'05 Workshops, Aug 2005.

[3] K. Fall, “A Delay-Tolerant Network Architecture for Challenged Internets,” Proceeding of Annual Conference of

the Special Interest Group on Data Communication (ACM SIGCOMM'03), pp. 27-34, Aug. 2003.

[4] Haojin Zhu, Suguo Du, Zhaoyu Gao, Mianxiong Dong, Zhenfu Cao, "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in delay-Tolerant Networks," IEEE transactions on Parallel and Distributed systems, vol. 25, No. 1, pp.22-32, January 2014.

[5] E. P. C. Jones and P. A. S. Ward, "Routing Strategies for Delay-Tolerant Networks," Submitted to Computer Communication Review (under review), 2008.

[6] A. Balasubramanian, Brian N. Levine and A. Venkatramani, "DTN Routing a Resource Allocation Problem," in Proceeding of ACM, 2007,pp .373-384,2007.

[7] Rongxing Lu, Xiaoding Lin, Haojin Zhu, Xuemin Shen, Bruno Preiss, "Pi: A Practical Incentive Protocol for Delay Tolerant networks," IEEE Transaction on wireless communications, vol. 9, No. 4, pp. 1483-1493, April 2010.

[8] F. Templin, Ed, S. Burleigh, "DTN Security Key Management - Requirements and Design", April 2016. draft-templin-dtn-dtnskmreq-00.txt.

[9] D Sarawagya Singh, Elayaraja.K, "Survey Of Misbehaviors Of Node And Routing Attack In Delay Tolerant Network", International Journal of Science, Engineering and Technology Research (TJSETR), Volume 4, Issue 2, February 2015.

[10] Ardra. P. S, A. Viswanathan, " A Survey On Detection And Mitigation Of Misbehavior In Disruption Tolerant Networks", IRACST - International Journal of Computer Networks and Wireless Communications (TJCNWC), Vo1.2, No6, December 2012.

[11] Afroze Ansari, Dr.Mohammed Abdul Waheed, "Novel technique for Black-hole Gray-Hole Detection under DTN, A Protocol Design Study", International Conference on Intelligent Computing and Control Systems ICICCS 2017.

[12] Shou-Chih Lo, Nai-Wun Luo, Jhih-Siao Gao, Chih-Cheng Tseng "Quota-Based Multicast Routing in Delay-Tolerant Networks" Wireless Personal Communication, 2014.

[13] William D. Ivancic, "Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks" IEEE, 2010.

[14] Lie Li, Hefei, Qiyue Li, "A price-based interactive data queue management approach for delay-tolerant mobile sensor networks" Wireless Communications and Networking Conference Workshops (WCNCW), IEEE, 2013.