Attack Detection And Its Analysis In DTN Mobile Ad-Hoc Network

Prachi Tiwari, S. Vennadhari

Abstract: The attacker in network at any cost degrades the routing performance. The routing of data in network is necessary for delivering data between the mobile nodes. In Delay Tolerant Network data is transferred in bundles. A mobile node whose participate in route will store the incoming data and forward to next connected mobile nodes when they also participate in route and available for data receiving. Delay tolerant routing should naturally support unicast and multicast routing strategy. Wireless mobile ad-hoc communication is topology less service because it performs in movable node environment. While the group communication established between nodes that new node register itself in the network and authentication provided by coordinator node after that node participate for any type of communication i.e. data sending or receiving. In this work we have actually measured the routing performance of DTN, Black hole attack, Jamming attack and Vampire attack. The performance of routing was compared with each other through performance metrics. In this network each type of attacker had different malicious activity. The malicious function of attacker was affected easily in this kind of decentralized network. Only these three attacker performance was measured in present work and the performance showed the disruption in normal routing performance. The presence of attacker also consumed the limited energy resource and this resource utilization improved network life. Thus DTN is the effective approach in routing of data in between sender and receiver. The attacker performance measurement provides the information about the attacker effect in dynamic network only.

Index Terms: DTN, MANET, Routing, Attack, Blackhole Attack, Jamming attack, Vampire Attack

1 INTRODUCTION
Mobile ad-hoc delay tolerant network (DTN) is a small group of node whose cooperative communicate with each other’s. DTN is a special purpose network because it supports interoperability between networks that minimized network delay using bundle based multicasting. Delay tolerant network save the network resource in terms of energy, queue, bandwidth and processing capability. Group communication in delay tolerant network (DTN) wireless mobile ad-hoc network are challenging issue because mobile devices or nodes freely move in the environment and are unsecure, because no any centralized security methodology exists in the past work. Reset of paper describes the work of attacks in different layer and its impact and also developed a new multi-layer secure multicast routing algorithm for Delay Tolerant MANET communication. Our multi-layer security mechanism identifies in-activity in every layer and highly secures the data from unauthorized user and false route. Our methodology worked under the group communication, but group communication is big challenge in MANET because maintenance of group members is crucial part for MANET, the problem of maintenance of group members using multicast MANET routing and efficient channel utilization was resolved by applying bundle based DTN service architecture. This approach provides are feasible and secure group communication in DTN mobile ad-hoc network.

2 LITERATURE SURVEY
S. C. Lo, N. Luo et. al. [1] Present a work on multicast quota based routing for delay tolerant network that work improve the higher data delivery rate and need not require to maintain the group members in unstructured network. Through their contribution node freely join and leave the network without priory intimation to the administrator. William D. Ivancic [2], work in the field DTN security and proposed a delay tolerant network security architecture with bundle based data transmission for the space based network, in this work they provide security for the routing decision time and sends data in secure manner to the destination. They focus the bundle safety at the same time as group communication engage, further each layer protection are inherent from given work and add to the privacy and reliability of the DTN communication. Jie Li et. al [3] has resolve the problem of queue management under the delay tolerant mobile ad hoc network in this work the addressed the priority assignment problem for the communication while compete multiple sender for same router node or intermediate nodes mean while they solve the priority assignment mechanism using price based method and sends the data prioritized based mechanism. 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. Xiaoming Tao et. al [4] proposed a algorithm for dynamic priority strategies under DTN multicast communication. In this approach end user behavior adjust based on priority, that work use full for congestion controlling under multicast communication in wireless sensor network, further that inbuilt with security with quality of service issue related problem resolution while denial of service occurs in the network. S.Karthika et. al [5] has a title provide the security with the help of fuzzy logic methodology under the DTN communication. Fuzzy rule takes the discrete input value i.e. node mobility, QoS, security and based on that set the trust value to all of nodes and select the trusted path for the communication. In this title, they analyse the problem of blackhole attacks in zone

* Prachi Tiwari, Deptt Of Computer Application, Rabindranath Tagore University, Bhopal, India, 464993, prachi.38@gmail.com
* S. Vennadhari, Deptt of Computer Application, Rabindranath Tagore University, Bhopal, India, 464993, veenadhari1@gmail.com
routing protocol in network. But not concerned about multicast communication based security so far the proposed approach tested through multilayer security based multicast communication in DTN network. Kevin Fall [6] works in the field of DTN and explain about challenges to designing the DTN network architecture under dynamic conditions in his work modify the working architecture of DTN for updates their basic service strategies and system interfacing. This is a comparatively essential approach; other than that approaches aim to restore underlying link performance problems or alter limited portions of the Internet architecture, such as routing decisions, with additional protocols in an effort to keep the current service model and existing TCP/IP based protocols constant. Because it provides various types of network services than the internet, the DTN design makes a different set of choices in the architectural design space: messages versus packets, a form of hop-by-hop reliability and protection versus end-to-end, name based routing versus address based routing, and a routing abstraction of partially-connected rather than fully-connected network graph. Interestingly, DTN can be covered upon the TCP/IP based Internet easily, and therefore remnants well-matched. In this title he focuses to design architectural model for internet communication and further modified by security related issue based mechanism and protect data from unauthorized users. Eugene Y. Vasserman et. al [7] proposed a methodology to defense the energy utilization through vampire attack under sensor ad hoc network communication. In his work they explore resource depletion attacks or vampire attack at the routing layer, which permanently disable networks by quickly draining nodes energy. They find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages. In the worst case, a single Vampire can augment network-wide energy practice. In this title they focus vampire attack detection and prevention whose reduce the energy of the nodes further enhanced that work by implementing multi-layer security based vampire attack detection and prevention, so no any attacker nodes are utilized unwanted energy resource of the nodes. Jerzy Konorski et. al. [8] are design an algorithm to secure the network through remapping attack. In this work author describe about how the traffic remapping attack change the priority order of the data packets and gain the network available resource such as queue, processing capability of devices and energy etc. traffic ramping attack consist in claiming a higher traffic priority, i.e., false designation of the intrinsic traffic class so that it can be mapped onto a higher-priority class. In practice, TRAs can be executed in IEEE 802.11 ad hoc networks using the Enhanced Distributed Channel Access (EDCA) function. This attack is easy to perform yet hard to prevent. For traffic ramping attacks prevention, they propose a distributed discouragement scheme based on the threat of TRA detection and punishment. The scheme does not rely on station identities or a trusted third party, nor does it require tampering with the MAC protocol. In further that work is useful for priority based arranging of network data so malicious node easily identified and punished. S. Abbas et. al. [9] Designs the security module against Sybil attack for the mobile ad hoc network. In this title, they proposed received signal strength (RSS) based detection mechanism to safeguard the network against Sybil attacks. The scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware. They established through a variety of experiments that a discovery threshold exists for the distinction of legitimate new nodes and new hateful identities. They confirmed this distinction rationale through simulations and through the use of a real-world test bed of Sun SPOT sensors. They also showed the various factors affecting the detection accuracy, such as network connections, packet transmission rates, node density, and node speed. The simulation results showed that our scheme works better even in mobile environments and can detect both join-and-leave and simultaneous Sybil attackers with a high degree of accuracy. Sybil attacker work under the MAC layer so in future work Sybil attack is also detect and prevented by our multi-layer security based approach and identifies the two different types of Sybil attacker present in the network. H. Mustafa et. al. [10] Designs a protocol for the jamming attack protection under multipath routing environment. In that approach established the multiple routes from source to receiver and calculates the path trust for the reliability identification of each path. That work helps to improve the security against active attack protection. That proposed methodology useful for congestion control and load balancing while rush of data traverse in the network. Further we elaborate that proposal by apply methodology under multicast group communication in MANET. Akshai Aggarwal, Savita Gandhi et. al. [11] has retrieve the node trust for the security analysis in mobile ad hoc environment that strategies is a improve version of ad hoc on demand distance routing protocol. Through the trust calculation increase the network reliability and security against attacker node from the network. That proposed work calculate the trust value of the node not only attack packet based it is also count the drop of data by MAC error, collision, congestion, route error etc. and that is not feasible for MANET communication because communication related error dropped data are not minimize so in further we apply attack symptoms based data drop for trust calculation of node and enhanced their work by multi-layer security based technique. S. Ramaswamy et. al. [12] proposed a methodology for detection and prevention of collaborative blackhole attack under mobile ad hoc network. In his method they define the cooperative blackhole attack symptoms and how does remove from the network under the ad-hoc on demand routing approach. Through that technique avoid the multiple blackhole attacker nodes from the network and secure the network communication. In this title the protect cooperative blackhole attack in MANET using one to one identification of node in every time that is routing layer attacker, further that work enhanced through the historic based data analysis and minimized the overhead on the preventer node on the network. N. Song and Lijun Qian et. al. [13] has design an algorithm for detection of wormhole attack under mobile ad hoc network. In his work apply the static analytic method to measure the network performance with multipath routing under wormhole attack impacts and its defensive mechanism. That is a simple scheme based on statistical analysis (called SAM) is proposed to detect such attacks and to identify malicious nodes. wormhole attacker node is
collaboratively spread the attack in the network so further we detect and prevent that attack by path tracing based approach so no any two node are coordinate communicate and spread the attack in the network, that functionality we apply in our proposed multi-layer security mechanism. Xiang Fa Guo [14] proposed an efficient routing for delay tolerant network whose apply the plankton methodology. Plankton creates the replicated message and decreases the control message overhead and achieves the excellent delivery ratio without loss of data packets. Kwan Wu Chin [15] develops a methodology and to achieve the high data delivery ratio for DTN bundle with low possible bandwidth availability condition. B. Abdali, M. Bouguig [16] explores the delay tolerant network through resource utilization predictability and manages the all needed resource for the communication. Their method improves the network performance in terms of bandwidth utilization, percentage of data delivery, throughput. They also compare the performance of existing core routing of mobile ad-hoc communication and found that their methodology is adoptable for current trends of network. M. Rahmatullah at. el. [17] proposed the feasible method for buffer management while the bandwidth variation within the network. Their technique two function are used bundle protocol and message forward method. Bundle protocol is special kinds of protocol which manage the buffer size of nodes and found that buffer overflow occurs than increase the buffer size for storing the new arrival data. After that forward to the next hop, that work better utilized the resource of the network and improve the network efficiency for the communication. S. Grover et. al. [18] work for delay tolerant network security, in his work defines the various security issues and its defensive mechanism for better throughput achieving. Security is a very challenging issue for the communication because attacker are different categories that is passive and active way present in the network and disrupt the designed communication backbone. Grover and their team design the defensive mechanism and to protect from attacker nodes, through their approach improve the network performances in all respect of network criteria. D. Pan et. al. [19] proposed the scatter and wait with probability choice base routing that provide efficient routing decision for the communication that also work as situation based routing decision and communicate them. Through probability based routing improves the packet delivery ratio and throughput of the network.

3. METHODOLOGY

In DTN the multicast approach was use and this approach was efficient than the normal multicast approach because in DTN data is delivered in network in bundle form and these bundles of messages also enhances the bandwidth utilization. The attackers are malicious nodes that are disturbing the original routing performance of network. The attackers also work on multiple layers of network and on each layer attacker aim is to affect the data of sender. The Blackhole attacker drops the data by generating the wrong route information of receiver existence. If the attacker identifies the sender, then in that case it is also possible to drop the data through fake id. This means Sybil attacker drops the data through fake id and this id is captured by attacker. On the other side some of the DoS attackers also had infected network by flooding of unwanted packets in network and those attackers consumes the valuable communication resources because communication overhead enhances. The jamming of data is a type of denial of service (DoS) attack, just difference is that jamming attack is identified at physical layer by observing the behaviour of signals or number of bits received at destination. The normal DTN routing showed better performance as compared to blackhole attacker, Sybil attacker, DoS attacker and Jamming attacker. The efficient bundle based technique is showing the degradable results in presence of multiple attackers and these attackers are showing the degradation in performance as compare to normal DTN performance. The behaviour of blackhole attacker is creating the routing loop.

```java
if (data_pkts_forwarding == false) && (node == next to sender)
    
    attacker is blackhole

} Same as the attacker presence of Sybil also drop the data packets but the technique of dropping data packets are different as compare to other packet dropping attacker.

    if (node_id != fake_id)
        if (data_pkts_forwarding = =False)
            
            Sybil attacker is confirming in network

} In DoS attacker in network is flooded huge amount of unwanted data from the communication network those data packets will arriving in each communicated node in network but these packets are consume the limited bandwidth of wireless network because of that the the data packets forwarding in between sender and receiver is affected. The behaviour of DoS attack is like

    if (pks= = message) && (message= null)
        
        attacker is DoS attacker

} Same as at physical layer the behaviour of jamming attack is

    if (bits= = message) && (message= null) // bits are not containing any information of route or data.

    Attacker is jamming attacker
```

Here the attackers are not detected by any security scheme but also the affected of attacker in DTN is shows and in shorts the attacker what kind of information drop or flooded in network shows in performance. e attacker presence shows degradation in performance due to this packet dropping and routing overhead is enhanced. The attacker’s symptoms will not have identified in network only performance of network in presence of different attackers are evaluated and identified the performance of attackers are showing deprivation as compare to normal DTN performance

4 SIMULATION PARAMETERS

The simulation of protocol is to provide the nearby accurate performance of any protocol in network. The performance
parameters used for simulation is given in table 1. The present work the routing protocol used for simulation is AODV. Radio range of nodes were 550 meters and modes moves in network through random way point model. The performance of protocol is measured in different node density scenario in dynamic topology.

**TABLE 1**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of Mobile Devices</td>
<td>25, 30, 35, 40, 45, 50</td>
</tr>
<tr>
<td>Network Size for simulation</td>
<td>800 * 800</td>
</tr>
<tr>
<td>Network Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Analysis time in seconds</td>
<td>100Sec</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>UDP/TCP</td>
</tr>
<tr>
<td>Data Type</td>
<td>FTP/CBR</td>
</tr>
<tr>
<td>Network Packet Size in Byte</td>
<td>512</td>
</tr>
<tr>
<td>Antenna Type</td>
<td>Omni Antenna</td>
</tr>
<tr>
<td>Node Speed (m/s)</td>
<td>Random</td>
</tr>
</tbody>
</table>

5 SIMULATION RESULT ANALYSIS
This section describes simulation analysis result through various parameters, applied for network simulator-2 and generated confusion metrics, network depended analysis etc.

5.1 PDR Performance Analysis
In the Graph 1 PDR performance of network analyze under attacker condition and delay tolerant bundle based group communication scheme, through the result defined that.

While the presence of attacker the data does not reaches destination in presence of blackhole attacker but jamming and vampire case the network resources like bandwidth and energy is consumed. In figure 1 the PDR performance of DTN, jamming attack is about 85% and 82% in network but in case Blackhole attack and Vampire attack performance is about 48 % and 40%.

5.2 Throughput Performance Analysis
The mobile nodes in DTN create the bundle and sends to all group receive node with low overhead method it also controls and manage the group of nodes whose cooperate for the group communication. The through performance in figure 2 is measured in per unit of time. The routing protocol group communication is based on specific bundle based communication between the sender and receiver. The throughput performance of DTN, Blackhole attack, jamming attack and Vampire attack is measure in DTN network. Here the throughput is DTN and Jamming attack is about 480 bits/sec and 410 bits/sec and the performance of rest of attacker like Blackhole attack and Vampire attack is about 240 bits/sec and 200 bits/sec.
5.4 Network Summarized Performance

The performance of DTN, Blackhole attack, jamming attack and Vampire attack is mentioned in Table 2 and observe that the performance of all attacks is measure through different performance metrics. Some criteria are nil in networks because the packet capturing due to attacker is not possible because no security scheme against attack is applied on network. The Table 1 is only shows the effect of attacker.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>DTN</th>
<th>Blackhole</th>
<th>Jamming</th>
<th>Vampire</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEND</td>
<td>5493</td>
<td>5494</td>
<td>5494</td>
<td>5493</td>
</tr>
<tr>
<td>RECV</td>
<td>4935</td>
<td>2682</td>
<td>4679</td>
<td>2196</td>
</tr>
<tr>
<td>ROUTINGPKTS</td>
<td>6599</td>
<td>5735</td>
<td>172785</td>
<td>90596</td>
</tr>
<tr>
<td>Blackhole Attack Capture</td>
<td>Nil</td>
<td>1613</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>Jamming Attack Capture</td>
<td>Nil</td>
<td>Nil</td>
<td>273870</td>
<td>Nil</td>
</tr>
<tr>
<td>Vampire Attack Capture</td>
<td>Nil</td>
<td>Nil</td>
<td>Nil</td>
<td>153898</td>
</tr>
<tr>
<td>Average Energy Consume</td>
<td>Nil</td>
<td>Nil</td>
<td>Nil</td>
<td>27.65</td>
</tr>
<tr>
<td>Average Residual Energy</td>
<td>Nil</td>
<td>Nil</td>
<td>Nil</td>
<td>62.35</td>
</tr>
<tr>
<td>PDF</td>
<td>89.84</td>
<td>48.82</td>
<td>85.17</td>
<td>39.98</td>
</tr>
<tr>
<td>NPR</td>
<td>1.34</td>
<td>2.14</td>
<td>36.93</td>
<td>41.26</td>
</tr>
<tr>
<td>Average e-e delay(ms)</td>
<td>16.95</td>
<td>18.35</td>
<td>30.77</td>
<td>22.64</td>
</tr>
<tr>
<td>No. of dropped data (packets)</td>
<td>558</td>
<td>2812</td>
<td>815</td>
<td>3297</td>
</tr>
</tbody>
</table>

6 SUMMARY OF WORK AND FUTURE PROSPECTS

DTN bundle of messages delivery provides efficient results in case of multicast communication in DTN-MANET. Portable device or mobiles have limited energy, processing capability and bandwidth capacity for communicating with other in dynamic network. In unicast communication, the data is only delivering to single destination. Group communication in mobile ad-hoc network perform by MAODV or ODMRP routing that acquire the path between group member node by sharing route information through all of member nodes that minimize the control message overhead of the network. The control overhead problem in presence of jamming and vampire attack is crosses the limits and this limit are counted in lacks number of packets. The energy is the most important factor required for communication in between sender and receiver. The unwanted packets flooding and dropping of packets also consumes the limited energy resource because of that the data sending quantity and receiving quantity is affected. The quantity of flooding also reduces the mobile nodes processing capability and limited bandwidth capacity. The attacker loss and network degradation is calculated through different performance metrics and these metrics are clearly shows the effect of attacker. The bundle of messages is forwarded in network through intermediate node and each node continuously moves in network with different speed. It is proposed to develop a security scheme against Blackhole attack, Jamming attack and Vampire attack. The attacker detection and prevention is possible by reliable security scheme. The proposed security scheme will provide the reduction end to end delay, routing overhead and rest of the performance.

REFERENCES

[9] Sohail Abbas, Madjid Merabti, David Llewellyn-


