Implementation and Analysis of Selective Forwarding Attacks in Wireless Sensor Networks

*Sachin Kumar, *Prince Singh, *Prashubh, ¹Ranjit Kumar, ¹Javed Miya

*Student, Information Technology Dept. Of Galgotias College of Engg and Tech. , Greater Noida, Uttar Pradesh, India

¹Assistant Professor, Information Technology Dept. Of Galgotias College of Engg and Tech. , Greater Noida, Uttar Pradesh, India

ABSTRACT

Wireless Sensor Networks (WSNs) are an emerging technology which are used in different applications, and thus become an interesting field of research. That is why security is a crucial issue and service in WSNs because wireless sensor nodes are typically deployed in unattended environments, leaving them open to possible hostile network attacks. Mobile adhoc network (MANET) is a wireless network of mobile devices without any infrastructure. An important problem receiving increased consideration recently is load balancing. Many protocols are developed under non uniform load distributions for improving bandwidth, energy efficiency, throughput etc. Mobile nodes in the network move and change its topology frequently. MANET are becoming increasingly common, and typical network loads considered for MANETs are increasing as applications evolve. One of the fundamental issues in a mobile adhoc network is the load balancing problem. Load balancing is a method for distributing workloads across computing resources. Load balancing is to provide a single Internet service from multiple servers is the commonly used application. Load balancing is transfer load balancing is the main field in mobile adhoc networks. In many previous works, supporting multicasting services at the link layer is essential for the efficient use of the network resources, since this approach eliminates the need for multiple transmissions of an identical payload while sending it to different destinations. In this project the system propose a light weight dynamic channel allocation scheme for MANET. The system compare two algorithms DCA-TRACE and CMH-T RACE to provide support for non-uniform load distributions and propose CDCA-TRACE. It increase the number of source nodes and reduce the number of collisions, energy consumptions and average absolute IPDV drastically.

KEYWORDS:-WSNs, Compromised node, Attacks, Security, MANETs. Ad hoc network security. Intrusion detection & prevention. Secure routing..
1. INTRODUCTION

Efficient use of the resources in mobile ad hoc networks (MANETs) is of great importance to maintain the required quality of service and to prolong the network lifetime. The utilization of the resources such as bandwidth and energy depends on a number of conditions such as network size, node density, and load distribution. These conditions are uncontrollable and often vary throughout the operation of the network. In order to efficiently use the resources, the protocols that determine the behavior of the network should dynamically adapt to these changing conditions. My thesis is that a protocol architecture for MANETs that dynamically adapts to changing conditions based on cooperation and information sharing leads to more efficient use of the system resources compared to competition based architectures. In particular, in this dissertation we explore the benefits of adaptation based on cooperation and information sharing at the medium access control (MAC) and network (routing) layers of the protocol stack. At the MAC layer, we develop an analytical model that reflects the relationships between protocol parameters and the overall performance of the protocol under various network conditions. This model reveals that the protocol parameters at the MAC layer can be adjusted to make best use of the channel resources depending on the application requirements and network conditions obtained through information sharing, such as average network load density. In order to provide a dynamic system that adapts not only to changing conditions but also to spatially non-uniform traffic load distributions, a lightweight dynamic channel allocation algorithm and a cooperative load balancing algorithm that facilitate efficient use of resources based on local information sharing are proposed. Through extensive simulations, we show that both dynamic channel allocation and cooperative load balancing improve the bandwidth efficiency under non-uniform load distributions compared with protocols that do not use these mechanisms as well as compared with the IEEE 802.11 uncoordinated protocol. Properly routing the data over a MANET is another challenging topic due to the dynamic behavior of the network, yet it is also crucial in terms of efficient use of resources. Two important routing schemes, network-wide broadcasting and multicasting, are investigated for trade-offs and merged into a single frame-work. The framework allows the selection of the optimal routing scheme based on the network conditions obtained through information sharing, leading to the best use of the system resources in terms of spectrum efficiency and energy efficiency. The interaction of a network with other networks coexisting at the same site also strongly determines its efficiency. We developed an approach for symbiotic networking using hybrid nodes, and our results clearly show that symbiotic networking can provide vital support to co-located networks, which is especially important in resource-constrained networks such as MANETs. Although theoretical analysis and simulations are efficient tools to comparatively evaluate the efficiency of different protocols, they cannot reflect many of the challenges for real implementation of these protocols, such as clock-drift, synchronization, imperfect physical layers, and interference from devices outside of the system. Mobile ad hoc networks (MANETs) are self-configuring mobile devices with no infrastructure. Each node in a MANET acts as a router and has capability to deploy anytime and anywhere. The application of mobile adhoc network are military, disaster management, industry and many more. Some characteristics of mobile adhoc networks are dynamic topology, distributed operation multi-hop routing. Mobile nodes in the network move and change its topology frequently. MANET are becoming increasingly common, and typical network loads considered for MANETs are increasing as applications evolve. One of the fundamental issues in a mobile adhoc network is the load balancing problem. Load balancing is a method for distributing workloads across computing resources. Load balancing is to provide a single Internet service from multiple servers is the commonly used application. Load balancing is transfer load balancing is the main field in mobile adhoc networks. Mobile ad hoc network have been an important class of network, providing communication support in mission critical scenarios including battlefield and tactical missions. This, in turn, increases the importance of...
bandwidth efficiency while maintaining tight requirements on energy consumption delay and jitter. Coordinated channel access protocols have been shown to be well suited for highly loaded MANETs under uniform load distributions. However, these protocols are in general not as well suited for non-uniform load distributions as uncoordinated channel access protocols due to the lack of on-demand dynamic channel allocation mechanisms that exist in infrastructure based coordinated protocols. There are many dis-advantage in the existing scenario of load balancing concept some of the disadvantage are, although sensor networks are being increasingly deployed in many application domains, assessing trustworthiness of reported data from distributed sensors has remained a challenging issue. Sensors deployed in hostile environments may be subject to node compromising attacks by adversaries who intend to inject false data into the system. In this context, assessing the trustworthiness of the collected data and announcing decision makers for the data trustworthiness becomes a challenging task. As the computational power of very low power processors dramatically increases, mostly driven by demands of mobile computing such technology drops, WSNs will be able to afford hardware which can implement more sophisticated data aggregation and trust assessment algorithms. Example is the recent emergence of multi-core and multi-processor systems in sensor nodes. To overcome the existing concept we include some of the concepts they are, in this paper we propose two algorithms to cope with the non-uniform load distributions in MANETs: a light weight distributed dynamic channel allocation Algorithm based on spectrum sensing, and a cooperative load balancing algorithm in which nodes select their channel access providers based on the availability of the resources. We apply these two algorithms for managing non uniform load distribution in MANETs into an energy efficient real-time coordinated MAC protocol, named MH-TRACE. In MH-TRACE, the channel access is regulated by dynamically selected cluster heads (CHs). MH-TRACE has been shown to have higher throughput and to be more energy efficient compared to CSMA type protocols. Although MH-TRACE incorporates spatial reuse, it does not provide any channel borrowing or load balancing mechanisms and thus does not provide optimal support to non-uniform loads. Hence, we apply the dynamic channel allocation and cooperative load balancing algorithms to MH-TRACE, creating the new protocols of DCA-TRACE, CMH-TRACE and the combined CDCA-TRACE. Mobile ad hoc networks (MANETs) can be arranged in various situations but the presence of variable degree of resources, movement of nodes and the lack of load-balancing competences in MANETs (Mobile Ad Hoc Networks) poses a large challenge for such networks to scale. Load imbalance is one of the critical issues in these networks and network performance can be reached by fairly allocating load among nodes within the network. In the given paper, special devotion has been given to the load balancing and congestion control in network. The various load-balancing schemes are discussed gives an ability to improve congestion by distribution of traffic of excessive load and to support better performance, taking different parameters into consideration. Ad hoc networks have gained more attention these last decades, with the explosion of mobile processing stages and small sized wireless tools. MANETs hold the promise of future, with the ability to launch networks at anytime, anywhere without assistance of any central authority. All the nodes are mobile but possess their own set of capabilities including their communication and computation power, energy resources etc., thus offer heterogeneity among nodes. Thus, a mobile ad hoc network (MANET) can be defined as an autonomous distributed system where node communicates over moderately bandwidth-constrained wireless links with other nodes which resides within its transmission range. Multi-hoping improves the problem of limited radio spread range and thus is an imperative feature of mobile networks. Limited security, dynamic topology, variable rate and limited bandwidth of connections and power consumption are some of the new limits imposed by ad hoc networks. Packet transmissions suffer from interference and fading due to the shared wireless channel and dynamic topology. As the demands for the support of multimedia communication has been increasing recently, bandwidth intensive, large amount of real time
traffic tends to be in bursts and is liable to congestion. MANETs enable one or more mobile units to communicate with each other without the survival of physical connection and any established infrastructure. All nodes have to make decisions jointly. In such environments imbalance of load over the nodes can occur. The competences of a MANET node is a function of its resources, battery power etc. A powerful node finishes its allotted jobs quickly and becomes idle before a less powerful node, allotted with extra work load or engaged most of the time, consuming more energy. The flow of data between the source and the destination nodes could be speed up if its efficiency split on multiple paths between them. Load balancing is surely one of the solutions for refining the efficiency of the applications and the life of the network nodes i.e. network lifetime. The significance of an efficient load balancing technique is to minimize the difference between the overloaded and under loaded nodes in terms of their workload by keeping other parameters in consideration. As these parameters changes time to time using different parameters, the process of balancing the network becomes more complicated. Imbalance of load in mobile networks results in packet dropping, end to end delay, inefficiency and imbalanced energy consumption. MANET has a dynamic network topology, and constraint resources, such as bandwidth, buffer space, battery and transmission power and so on. Distributing traffic fairly among the mobile hosts, based on measurement of path statistics, is beneficial in order to take full advantage of the limited resources and to use network resources better so that the congestion and end-to-end delay are minimized. Load balancing schemes allocate the network loads, which can prevent network from getting into the state of congestion, and avoid the resources of congested node to be drained. The routing algorithms in MANET that choose the shortest route to build up the communication path may incur traffic imbalanced problems in the network. During data communication the interference between two or more multiple paths located physically close enough to interfere with each other, refers to route coupling. Routing is the process of selecting the best path in the network. Here it is focused on routing layer in order to increase the performance of the system. An Energy Aware Clustered algorithm based Routing is introduced which forms several clusters, finds energy aware node-disjoint multiple routes from a source to destination and increases the network life time by using optimal routes. Clustering is an important research area in mobile networks because it improves the performance of flexibility and scalability when network size is huge with high mobility. All mobile nodes operate on battery power hence the power consumption becomes an important issue in Mobile Network. Through the simulation with an enhanced version of NS-2 simulator Energy Aware Clustered algorithm shows the improvement in throughput, Energy Consumption and delay when compared to other algorithms. Mobile networks (MANETs) is a self-configuring mobile devices with no infrastructure. Each node in a MANET act as a router and has capability to deploy anytime and anywhere. The application of mobile network are military, disaster management, industry and many more. Some characteristics of mobile networks are dynamic topology, distributed operation multi hop routing. Mobile nodes in the network moves and changes its topology frequently.

Figure 1. Architecture of MANET and VANET
2. Related Work

Threat of collaborative attacks on MANETs is noticed by so many researchers. Hence, research in various defending mechanisms, preventive approaches are going on and result design of several mechanisms to defend against collaborative attacks done.

In [1] the author used a data routing information (DRI) table at each node and cross checking method to identify the cooperative black hole nodes in the network. The modified AODV routing protocol was used to achieve this methodology. The experiment results show that this solution performs better than other solutions.

In [25] the author presents the most important forms of attacks, discuss possible collaboration among various attackers and show how various signal processing and neural learning can help in detection and defense of collaborative attacks in such environments. They also showed how collaborative attacks can cause a worse effect on wireless than on a wired network. Experimental results demonstrate the validation and effectiveness of the model proposed by minimizing the collaborative attacks and immunizing the mobile ad hoc networks.

In [3] the author addresses the problem of collaborative insider attacks where critical data within the information systems is compromised by two or more insiders working together. Author first discussed about various relations among illegal information flow diagram and information system components. Then after, various characteristics of data accesses summarized by the mutual-access-record’s probability value and the transaction distance to data item are presented. Afterwards the algorithm is introduced for detecting collaborative insider attacks.

In [5] the authors analyze MANETs under single and collaborative Black Hole attack and proposed a technique to prevent it by diverting traffic from the Black Hole nodes. The MANETs so discussed make use of the AODV routing protocol and the method so proposed is based on sending confirmation packets that are verified by the destination to check for the Black Hole presence in the GAODV routing protocol so proposed.

In [20] the author proposed a theory that balanced Collaborative attackers can pass trusted nodes assistance methods which are very often used in existing secure schemes. On the basis of theoretical analysis, the reports so formed between BC attackers have the highest similarities ratio. They proposed an algorithm to check abnormality detection and to detect BC attackers. The bit error probability of secondary users is the only information they required to know of reporting channel. The Numerical simulation results show that the proposed technique can easily identify and find out BC attackers clearly.

3. Proposed Method EMAODV(Enhanced Modified AODV)

AODV can be extended by adding two types of control packets and threshold value: Secure Reliable Route Discovery Request (SRRD_REQ) and Secure Reliable Route Discovery Reply (SRRD_REP). SRRD_REQ messages are also known as control packets sent by the source node along with SRRD-ID as destination sequence number of destination node over the MANET on regular intervals and SRRD_REP message in response of SRRD_REQ by the destination to the source node after matching SRRD_ID. SRRD_REP can only be generated by the destination node as assumption which means there is no role of other nodes i.e. no node other than the destination, can generate SRRD_REP on behalf of the destination node. In addition, Routing table also contains new fields called Reliability List (RL) and Threshold Value (TV) as routing table entry. But no change in the format of EMAODV Routing Table entry compare to normal
AODV routing table entry except two additional fields RL and TV. RL (Reliability list) contains nodes that are trustworthy and TV contains average of all destination sequence number of reliable nodes. Path discovery compose of two phases: Phase I & Phase II discussed below.

- Algorithm For Enhanced Modify AODV

The algorithm for EMAODV to detect and prevent attacker nodes in MANET given below –

Phase I - When a source node in MANET wish to send data packets to any destination node within the network then firstly check whether there is any update route present in the routing table. If reliable route found then transfer data packet through it else initiate the route discovery process. In this process, the source forward SRRD_REQ to its neighbor nodes with SRRD_ID for creation of new route. When an intermediate node receives an SRRD_REQ it does the following steps:

x If this node has an updated route to the required destination, then it sends SRRD_REP to the source else broadcast the SRRD_REQ to its neighboring nodes with hop count incremented by 1.

x Sets up a reverse path discovery for the reply message.

x If the node having an entry in its routing table towards the source as destination but it is not updated enough, hence it refreshes it. If there founds an entry in RL (Reliable list) for the destination, then delete and update it also.

x If no entry found for the source in the routing table entries then creates new entry during reverse path technique. More than one reliable route found and arranges these routes according to minimum hop count. Then Compare first node destination sequence number of top reliable route with minimum hop count with TV (threshold value). If its value greater than average of DSNs of route nodes then it must be an attacker node so discard this route and check for another till no reliable route found having less DSN value then TV.

x Most Reliable route with minimum hop count is selected for new entry to the source node by copying the hop count, source sequence number from the SRRD_REQ packet and address of neighbor from which first received copy of broadcasting request or message packet, take as the next hop.

When the destination receives SRRD_REQ packet it sends back SRRD_REP using the reverse path. SRRD_REP may also be sent by some intermediate node which is having an updated path to the destination. During reverse route technique, each node that receives SRRD_REP performs the following steps:

x If that node contains an entry for the destination but not currently updated one, it updates that entry, else creates a new entry to its routing table.

x Also must appends an entry with IP address of source copied from originator field of SRRD_REP packet. FDPC and SRRD_ID are set to zero. Also forwards it to next hop on reverse route.

In AODV route discovery process done when originator receives Route REP messages. But in Enhanced Modified AODV, phase 2 starts from this point.
Phase 2 - Source node sends SRRD packets to all the nodes from which it got RREPs. Now every node which receives SRRD does the following:

- If there is a reverse path entry in its routing table for source, it sets SRR_ID by copying it from SRRD. Else, creates new entry.
- Now forwards packets to all those nodes from where it received SRRD_REPs earlier.
- Each node on the path of SRRD should be having an entry for the destination.

When the destination receives the SRRD packet it replies with SRRD_REP to its neighbour node from which it received the first SRRD packet and else discards others. The destination sets the reliability value in the SRRD_REP packet to 1. During reverse path technique, each intermediate node receives only one copy of SRRD_REP for the first time (SRRD_ID = 1) do two steps: sets FDPC to zero in SRRD_REP and then forwards it to the next hop on the reverse path. Finally, the source node gets SRRD_REP. After all no intermediate node can generate SRRD_REP, this SRRD_REP is unique and the path is discovered.

4. Simulation Environment and Graphical Results Analysis

In this section, we discussed about various simulation parameters, operations of proposed method EMAODV and lastly graphical results to be analysed.

Simulation Parameters-
The first phase of Simulation is to design a mobile Ad hoc network scenario which provides the workspace where the desired MANET is modelled. Predetermined parameters of NS2 and required attributes of node are configured. The entire system is built on some values and settings that we hope would enable us to provide more stable simulation results than before.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Initial value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation time</td>
<td>90 (s)</td>
</tr>
<tr>
<td>Sum of mobile nodes</td>
<td>23</td>
</tr>
<tr>
<td>Sum of static nodes</td>
<td>3</td>
</tr>
<tr>
<td>Sum of base-station node</td>
<td>1</td>
</tr>
<tr>
<td>Sum of blackhole nodes</td>
<td>3</td>
</tr>
<tr>
<td>Sum of grayhole node</td>
<td>2</td>
</tr>
<tr>
<td>Normal routing protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Blackhole and Grayhole attack protocol</td>
<td>blackholeAODV,grayholeAODV</td>
</tr>
<tr>
<td>Traffic</td>
<td>CBR</td>
</tr>
<tr>
<td>Normal packet size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Abnormal packet size</td>
<td>1024 bytes</td>
</tr>
<tr>
<td>Data rates</td>
<td>10 Kbits</td>
</tr>
</tbody>
</table>
By using NS2, same network is generated with 23 nodes having some nodes act as the Blackhole attack and Grayhole attack similar to normal AODV. The Connection so creates between source and destination is UDP. With the help of CBR (Constant Bit Ratio) application, Traffic is generated with constant packets through the UDP connection. Packet size of CBR seized to 512 bytes and set data rate to 10 Kbps. Similar scheme used for the simulation of UDP connection and traffic generation in EMAODV as in normal AODV.

Operations of Proposed Method EMAODV

Observations with changing Malicious Nodes ratio and fixed mobility-

In Fig. 2, we clearly observed that Normal AODV radically experience from Blackhole attacks and Grayhole attacks when malicious node percentage increases. This recognized the fact that Normal AODV doesn’t have any secure method to detect or prevent Blackhole and Grayhole attacks. The Proposed EMAODV scheme illustrates high packet delivery ratio compared with that of Normal AODV in different conditions (with no attacks, with Blackhole attacks only, with Grayhole attacks only and with collaboration of both Blackhole and Grayhole attacks). Also during the case where 50% of the total nodes in the network are malicious, the EMAODV proposed method still prevents or detects those malicious nodes successfully while keeping the packet delivery ratio above 85%.

![Figure 2. Packet delivery ratio of Normal AODV during different conditions and the EMAODV w.r.t. MNR](image)

In fig 3, we study about routing overhead of the EMAODV and Normal AODV with respect to MNR (malicious node ratio). The results show that when the total no. of malicious nodes increases, Normal AODV generates the lowest routing overhead contrast with the EMAODV. This recognized the fact that Normal AODV doesn’t have any secure method to detect or prevent Blackhole and Grayhole attacks.
In fig 4, the results are captured about average end-to-end delay of the proposed EMAODV and Normal AODV with respect to MNR (malicious node ratio). The results show that the EMAODV gains a little bit more avg. end-to-end delay as compared with Normal AODV. This recognized that the EMAODV requires more time to detect malicious nodes. Therefore, end-to-end delay and packet delivery ratio are inversely proportional to each other.

In fig 5, we examined the throughput of proposed EMAODV and the Normal AODV with respect to MNR (malicious node ratio). The results show that Normal AODV experiences the most from malicious-node attacks compared with the EMAODV. Also during the case where the total number of malicious nodes in the network is comparatively high (up to 40%) the EMAODV can still detect malicious nodes successfully while keeping the throughput above 14 000 bit/s.
Figure 5. Throughput (bit/sec) of Normal AODV and the EMAODV w.r.t. MNR

5. Conclusions

In MANETs considerable interest has recently been devoted to mechanisms that enforce security. Many proposals have been made in the literature to secure MANETs from various attacks, but most are attack-specific. Unlike some mechanisms that provide protection through authenticated routing, the Generalized Intrusion Detection & Prevention mechanism that we have proposed in this paper monitors both network layer characteristics (NCM) and performance statistics (DM). GIDP uses a combination of anomaly-based and knowledge-based ID that can protect MANETs against a variety of attacks. Simulation results of our case study show that our approach can protect MANETs from a wide variety of attacks with an affordable processing overhead. We also investigated the severity of various attacks and their impact on network performance along with the impact of the GIDP intrusion response on network performance. The results show that in some cases isolating the attacker can cause more harm than good to network, hence an adaptive flexible intrusion response mechanism is required. This will be our focus of research in future. In future work, the simulations can be developed for other combinations of attacks that are compatible to each other having their own specification to target the MANETs. Also find out different compatible collaborative attacks having own expertise that targets MANETs.

6. REFERENCES


