ISSN 2319 - 5975

Volume 1, No.1, July August- September 2012
International Journal of Networks and Systems
Available Online at http://warse.org/pdfs/ijns02112012.pdf

Secure DSR Protocol in MANET Using Energy Efficient Intrusion Detection System

Sneha Kumari[1], Dr. Maneesh Shrivastava[2]
[1]Department of Information Technology, LNCT, Bhopal, India, sneha.kumari3003@gmail.com
[2]Department of Information Technology, LNCT, Bhopal, India, maneesh.shreevastava@yahoo.com

ABSTRACT

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. In an attempt to enhance security in MANETs many researchers have suggested and implemented new improvements to the protocols and some of them have suggested new protocols. The attacks on MANET's challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. And also energy efficient routing is most important because all the nodes are battery powered. Failure of one node may affect the entire network. If a node runs out of energy the probability of network partitioning will be increased. Since every mobile node has limited power supply, energy depletion is become one of the main threats to the lifetime of the ad hoc network. The DSR protocol uses source routing rather than the hop-by-hop routing used by the majority of other protocols, which eliminates the need for frequent route advertisement and neighbor detection packets. In this paper we proposed secure DSR protocol in MANET using energy efficient intrusion detection system. The experimental results show that the effectiveness of our results is more efficient than existing works.

Keywords: MANET, DSR, Intrusion Detection, Energy Consumption.

1. INTRODUCTION

The most fundamental aspect of an ad hoc wireless network is its lack of infrastructure, and most design issues and challenges stem from this characteristic. lso, lack of centralized mechanism brings added difficulty in fault detection and correction. Home networks are envisioned to support communication between PCs, laptops, PDAs, cordless phones, smart appliances, security and monitoring systems, consumer electronics, and entertainment systems anywhere in and around the home. The dynamically changing nature of mobile nodes causes to the formation of an unpredicted topology. This topology change causes frequent route change, network partitioning and packet dropping. Because mobile nodes communicate each other via bandwidth-constrained, variable capacity, error-prone, and insecure wireless channels, wireless links will continue to have significantly lower capacity than wired links and, hence, more problematic network congestion. In MANET, network connectivity is obtained by routing and forwarding among multiple nodes. Although this replaces the constraints of fixed infrastructure connectivity, it also brings design challenges. Due to various conditions like overload, acting selfishly, or failed links, a node may fail to forward the packet. Misbehaving nodes and unreliable links can have a severe impact on overall network performance. Due to the lack of centralized monitoring and management mechanisms these types of misbehaviors cannot be detected and isolated quickly and easily. This increases the design complexity significantly. Mobile wireless networks are more vulnerable to information and physical security threats than fixed-wired networks. The use of open and shared broadcast wireless channels means nodes with inadequate physical protection are prone to security threats. Quality of Service (QoS) guarantee is very much essential for the successful communication of nodes in the network. The different QoS metrics includes throughput, packet loss, delay, and jitter and error rate. The dynamically changing topology, limited bandwidth and quality makes difficulty in achieving the desired QoS guarantee for the network. The main challenges are how to provide maximum lifetime to network and how to provide secure communication to network. As mobile ad-hoc network totally rely on battery power, the main aim for maximizing lifetime of network is to conserve battery power or energy with some security considerations [1] and [2] and [4].

In this paper we proposed first efficient intrusion detection technique for security and secondly proposed a new energy efficient dynamic source routing protocol which is based on the minimum-hop fixed-transmit power version of DSR.

2. BACKGROUND TECHNIQUES

2.1. Secure Data Routing in MANET

The main constrains of MANETs are the power, storage and processing these limitation and the specific architecture of sensors nodes call for energy efficient and secure

communication protocols. The key challenge in MANETs is to maximize the lifetime of sensor nodes because of, practically it is not possible to replace the batteries of large number of deployed sensor in the environment.
We focus on data-routing problems in energy constrained mobile ad-hoc networks. The main goal of data-routing algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. in our framework we have also consider some security issues to establish secured data routing in wireless sensor networks with negligible over head. Data routing techniques can significantly help to conserve the limited energy resource by eliminating data redundancy and minimizing the number of data transmission .for that reason, data routing techniques in MANETs are broadly investigated in the literature [3] and [5-6].

2.2. Energy Efficient Cluster-Based Approach

In cluster-based approach, whole network is divided in to several clusters. Each cluster has a cluster-head which is selected among cluster members. Cluster-heads do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to sink. The advantages and disadvantages of the cluster-based approaches is very much similar to tree-based approaches.
In recent, proposed a maximum lifetime data aggregation algorithm which finds data gathering schedule provided location of sensors and base-station, data packet size, and energy of each sensor. A data gathering schedule specifies how data packet are collected from sensors and transmitted to base station for each round. A schedule can be thought of as a collection of aggregation trees. In, they proposed heuristic-greedy clustering-based MLDA based on MLDA algorithm. In this they partitioned the network in to cluster and referred each cluster as super-sensor. They then compute maximum lifetime schedule for the super-sensors and then use this schedule to construct aggregation trees for the sensors.

In previous, present two-phase clustering (TPC) scheme. Phase I of this scheme creates clusters with a cluster-head and each node within that cluster form a direct link with cluster-head. Phase I of this scheme is similar to various scheme used for clustering but differ in one way that the cluster-head rotation is localized and is done based on the remaining energy level of the sensor nodes which minimize time variance of sensors and this lead to energy saving from unnecessary cluster-head rotation. In phase II, each node within the cluster searches for a neighbor closer than cluster-head which is called data relay point and setup up a data relay link. Now the sensor nodes within a cluster either use direct link or data relay link to send their data to cluster head which is an energy efficient scheme. The data relay point aggregates data at forwarding time to another data relay point or cluster-head. In case of high network density, TPC phase II will setup unnecessary data relay link between neighbors as closely deployed sensor will sense same data and this lead to a waste of energy.

An energy efficient and secure pattern based data aggregation protocol which is designed for clustered environment. In conventional method data is aggregated at cluster-head and cluster-head eliminate redundancy by checking the content of data. This protocol says that instead of sending raw data to cluster-head, the cluster members send corresponding pattern codes to cluster-head for data aggregation. If multiple nodes send the same pattern code then only one of them is finally selected for sending actual data to cluster-head. For pattern matching, authors present a pattern comparison algorithm [1] and [7] and [8].

2.3. Energy Efficient Location based approach

Location based routing uses the geographic position of nodes to make routing decision. Location information can be obtained through GPS or some other mechanism. One of geographical-based routing protocols is location-aided routing (LAR) [8]. The central point of LAR is the limited flooding of routing request packets in a small group of nodes which belong to a so-called request zone. To construct the request zone, the expected zone of the destination needs to be obtained first. The procedure of route discovery in LAR is: The source puts the location information of itself and the destination in the routing request packet. Then routing request packet is broadcast within the request zone. In other words, the nodes within the request zone forward the message, others discard the message. On receipt of the route request packet, the destination sends back a route reply packet which contains its current location; If LAR fails to find the route to the destination due to estimation error or other reasons, the routing protocol resorts to flooding of routing message throughout the MANET [9] and [10].

3. PROPOSED ENERGY EFFICIENT INTRUSION DETECTION SYSTEM

Secure energy efficient routing is very essential in MANET. We have observed the different approaches used to bring secure energy efficiency in routing. These approaches make them efficient but then also it can't go beyond a limit. This makes us for the search of new innovative approaches. Secure energy efficient routing techniques play a significant role in saving the energy consumption of the network. There are many existing MANET routing protocols as described above, each one is having its own advantages as well as disadvantages. After looking through the existing protocol, we decided to design a secure energy efficient routing protocol which reduces the total energy consumption in the network and thus maximize the life time of the network. We proposed first efficient intrusion detection technique for

security and secondly proposed a new energy efficient dynamic source routing protocol which is based on the minimum-hop fixed-transmit power version of DSR.

3.1. Proposed Efficient Intrusion Detection

The aim of intrusion detection systems is to detect attacks against computer systems and networks. Intrusion detection systems detect attempts by legitimate users of the information systems to abuse their privileges or to exploit security vulnerabilities and attempts by external parties to infiltrate systems to compromise private information, manipulate communications, or to deny service. There are two main designs available to IDSs for detecting attacks: 1) the misuse detection design and 2) the anomaly detection design.

Design of the Intrusion Detection Engine (IDE):

Now we describe an insight into the design of the Intrusion Detection Engine. Justification of the major design decisions is also given. The design of the IDE uses the object oriented paradigm. The problem was broken down into smaller components, and appropriate classes were developed to accurately represent the problem.
A major factor in the design of the IDE is the complexity of the environment being monitored. Within any enclave, we expect to monitor events interleaved from multiple:
→ Concurrent sessions
→ Different principals
→Different protocols

Architectural Design of IDE:

A number of issues had to be taken into account in the design phase of this research implementation. The design was created in order to ensure that all the requirements and specifications were satisfied. In the secure enclave it is possible to have multiple concurrent sessions of different protocols executing within the enclave. The sessions may consist of the same or different principals. The Intrusion detection engine must be able to keep track of the different protocol sessions executing within the enclave in order to detect any attacks or suspicious activity. Not all attacks on security protocols occur over a single session. As described earlier, multi-session attacks such as replay attacks or parallel attacks may occur within the enclave. These multi-session attacks span multiple different protocol sessions. The Intrusion detection engine must provide a means to keep track of such executing sessions and detect any attacks.

Additionally, the detection of attacks has to be communicated to the person or system monitoring the enclave. Detailed reports of all attacks or suspicious behavior must be generated by the IDE. Such reports provide in-depth information about the type of attack and principals participating in the protocol session. The Intrusion Detection Engine receives crucial inputs from the Activity Monitor and from the Knowledge base of protocol signatures. It is important to ensure that interfaces with the Monitor and the Knowledge base are well-defined and reliable.

The IDE receives protocol events from the monitor as they occur. The IDE is multi-threaded with a single thread to serve as the thread dispatcher. Since each protocol may have many attack signatures associated with it, when a new protocol session begins, the IDE spawns a new thread to monitor all the FSM recognizers for that protocol.

To keep track of all the threads existing within the system, a Thread List class is employed, that holds the protocol name, session number, identifiers of the principals involved a signal to which the thread listens, and a thread identifier for each thread.

Functionality of the Intrusion Detection Engine:

The threads provide the detailed functionality of the Intrusion Detection Engine. Each thread monitors the activity within a single protocol session. As events for a particular protocol session come in from the activity monitor, the thread matches those events against the protocol signatures stored in the knowledge base. If a event matches, the Finite State Machine corresponding to that particular signature is advanced to the next state.

Upon conclusion of an attack session or a normal protocol session, it may so happen that the entire signature from the knowledge base matches the succession of events for that protocol session coming in from the activity monitor. In such cases, the thread will raise alerts to the console, providing information about the attack or normal session. If an attack is detected by the Intrusion Detection Engine, the detailed information about that attack is written to a text file.

This information is used by the Graphical User Interface component of the IDE to generate the attack reports. Threads terminate in two normal ways: (1) An attack is detected, or (2) The protocol ends normally. However if a particular protocol session hangs with no further events coming into the IDE, the thread will die after a timeout period and it will signal the activity as an abnormal termination. When a thread dies, the corresponding entry from the list of threads designed as an object of the Thread List class is removed.
Threads are chosen as control structure of choice for the IDE for several reasons. First, the number of concurrent threads spawned by a process is limited only by the virtual memory on the system. This allows the IDE to track a large number of concurrent sessions, accurately representing an Internet environment that is rich with security protocols. Secondly, there are no synchronization issues to be taken care of as all

the threads have their own memory space and can also access the global variables. Any data structure that is accessed by all the threads has been protected by means of a critical section. The overall design of the IDE is reflected in the flow chart as shown in Figure1.

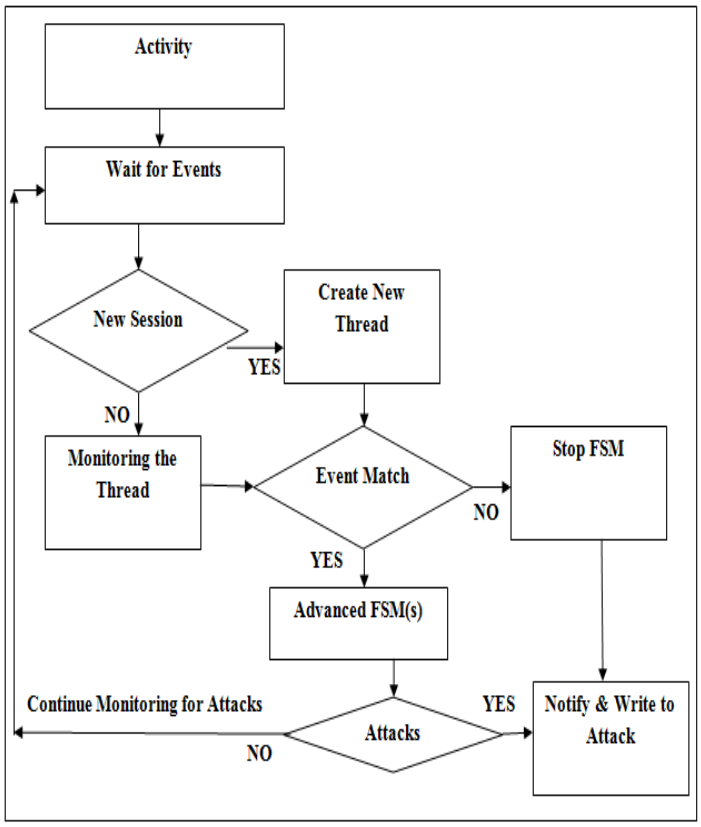

Figure 1: Flow Chart of Intrusion Detection Engine

In our work, a Graphical User Interface (GUI) was implemented for an overall view of the attacks and suspicious activities detected within the enclave. The GUI allows the reporting of attacks to the user. The user can specify the time duration and the protocol name to obtain a detailed report of all the attacks (on the specific protocol) that took place during that period. The report will include the name of the protocol subject to attack, the principals involved in the session, attack time and other relevant information which will allow the user monitoring the system to research the occurrence of attacks within the system.
The GUI also allows the user to back up the active attack report file to another file. The GUI will still read from both files to create the attack reports, but the IDE threads will only be writing to the newly empty active file.

The IDE is correctly able to report such activity as unrecognizable suspicious activity on the basis of its inability to find a complete match for that particular signature in the Knowledge base. It is always the case that protocol sessions successfully run to termination.

Proposed Energy Efficient Dynamic Source Routing Protocol

We have proposed an Energy Efficient Dynamic Source Routing which is based on Transmission power control approach and Load balancing approach. To reduce the transmission energy we are using a hop-by-hop power control mechanism and for load balancing it will select the nodes which are underutilized by avoiding the node which is having the least remaining power. Here during the route discovery phase itself we are calculating the minimum energy required to communicate to the node which sends the request to it. At the same time we observe each nodes remaining power to avoid a route which is having a tendency to die out. The destination node will make a decision about the selection of best route among the multiple requests that reaches to it and sends reply packet to the destination through the selected route. We avoid the additional computations required to find out the route as well as the multiple replies to the source. The minimum energy routing protocol is designed and implemented by making changes in the minimum-hop fixed-transmit power version of DSR.

To obtain an energy efficient routing protocol we uses power control approach and load balancing approach. In our proposed Energy Efficient DSR, a hop-by-hop power control mechanism is used to adjust the total power consumption of the network. To improve the lifetime of the network we avoid over utilized nodes and instead we select energy rich nodes to take part in routing.

In Energy Efficient DSR, the route which is having the tendency to break early is detected and avoided by adding a Min_Pow field in the RREQ packet. This Min_Pow field is used to hold the remaining battery power of a node. When a node accepts a RREQ packet from its neighbor it compares the Min_Pow value in the packet with its remaining energy. If the remaining power is less than Min_Pow, this power is assigned as the Min_Pow. This process will continue up to the destination. The destination which accepts more than one RREQ from different route, select the route which is having the highest value in the Min_Pow field and send RREP to the source. That means we are selecting a route by avoiding the node which is having a tendency to die out. This way we are removing the route which may break early. To save the remaining battery energy we uses a hop-by-hop control mechanism in which the nodes that receives a RREQ at power P_{recv} which transmitted it at P_{trmn} , calculates the new transmission power p_{new} for this receiving node such that this node can communicate with the sender by using this minimum required power P_{new} using:

$$P_{new}=P_{trmn}-P_{recv}+P_{threshold}+P_{margin}\ldots\ldots\ldots\ldots\ldots\ (1)$$

Where Pthreshold is the required threshold power of the receiving node for successful reception of the packet and Pmargin is the power included to overcome the problem of unstable links due to channel fluctuations. While sending back the RREP it sends the same power to the sender node and it uses this power for data packet transmission. The calculated power at each node is stored in a power table and this is the minimum required power for successful transmission and reception. The node rebroadcast the RREQ with maximum power, if it is not the destination. The next hope node also does the same procedure and it will continue up to the destination. The destination node may get more than one RREQ packet from different available route from the source. It will select a route which is having more energy in the RREQ packet so that it can communicate with the destination for a long time. It simply ignores the remaining request packet in the assumption that it cannot live for long time as compared to the selected one. So the selected route doesn't have a node that may early die out and is an energy efficient one since the hop-by-hop power control. Each pair of nodes in the rout will use the required transmission power for its successful communication. So the destination node will send a RREP packet to the source through the selected route and it reduces the overhead of multiple RREP.

4. RESULT ANALYSIS

Mobile ad-hoc wireless networks inherit the traditional problems of wireless communications, such as bandwidth optimization, power control, and transmission quality enhancement, while, in addition, their mobility, multi-hop nature, security and the lack of fixed infrastructure create a number of complexities and design constraints that are new to advanced secure mobile ad hoc networks. Our proposed Energy Efficient Secure DSR Protocol is successfully implemented using NS2 simulator, in which I have implemented the algorithm in existing techniques by making necessary changes in the existing system. We carry out quantitative and comprehensive evaluation of performance in terms of time, overall performance ratio, and traffic sensitivity. The simulation parameters of our thesis work is shown in following Table1:

Transmission range	***40-320 (M)***
No. of mobile nodes	***30-300***
Packet rate of normal connection	***1***
Movement Model	***Random Waypoint***
Traffic type	***CBR, HTTP, FTP***
Max. mode speed	***5 m/s – 30 m/s***
No. of connections between nodes	***5 – 30***
Topology Size	***200 X 200***
Pause time	***10 s***
Rate (packet per sec)	***2 packets/s***
Data payload (packet size)	***28 – 1024 bytes***

Table1 : Simulation parameters

The random waypoint model is chosen for movement patterns. In the random waypoint model of mobility, nodes choose a destination and move in a straight line toward the destination at a speed uniformly distributed between 0 meters/second (m/s) and some maximum speed. When a node reaches its destination, it stays during a specified period of time called pause time, chooses a new destination and begins moving towards it immediately in the same speed. Depending on number of connections and maximum node speeds. Number of connections implies here maximum number of connections between 200 nodes at a given time. Maximum speed of nodes indicates degree of mobility in the network. A static scenario of 2 mobile nodes was randomly distributed initially in an area of 200m by 200m (a square area). The source and destination pairs were spread randomly over the network but the numbers of pairs were kept constant during each scenario. Each CBR source started randomly at the beginning 0 to 10 seconds of the simulation and each simulation was run for 250 seconds. The number of connections was 2 in our case. We measured total energy consumptions of the nodes at the end of simulation.

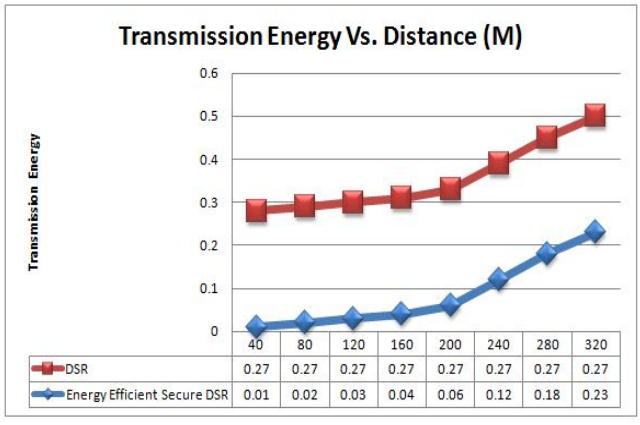

Figure 2: Transmission Energy Vs Distance (M)

The simulation result shows that the proposed energy efficient Secure DSR Protocol scheme uses transmission power according to the distance. If the distance is less, transmission power used is also less. On the other hand normal DSR need more transmission energy comparing our proposed scheme as shown in Figure 2.

CONCLUSION

Mobile wireless networks are more vulnerable to information and physical security threats than fixed-wired networks. The use of open and shared broadcast wireless channels means nodes with inadequate physical protection are prone to security threats. In addition, because a mobile ad hoc network is a distributed infrastructure-less network, it mainly relies on individual security solution from each mobile node, as centralized security control is hard to implement. And also energy constraints are another big challenge in mobile ad-hoc wireless network design. These constraints in wireless network arise due to battery powered nodes which cannot be recharged. This becomes a bigger issue in mobile ad hoc networks because as each node is acting as both an end system and a router at the same time, additional energy is required to forward packets.

There are many existing MANET routing protocols as described, each one is having its own advantages as well as disadvantages. After looking through the existing protocol, we decided to design a secure energy efficient routing protocol which reduces the total energy consumption in the network and thus maximize the life time of the network. We proposed first efficient intrusion detection technique for security and secondly proposed a new energy efficient dynamic source routing protocol which is based on the minimum-hop fixed-transmit power version of DSR. The experimental results show that the effectiveness of our energy efficient secure DSR is more efficient than normal DSR.

REFERENCES

1. C.Gnana Kousalya and Dr.J. Raja. **An Energy Efficient Traffic-Based Key Management Scheme for Wireless Sensor Network,** IEEE 2009 International Conference on Networking and Digital Society, pp.156-163.

2. Preetee K. Karmore and Smita M. Nirkhi, **Detecting Intrusion on AODV based Mobile Ad Hoc Networks by k-means Clustering method of Data Mining** , International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, pp 1774-1779.

3. Ashish Kumar, M. Q. Rafiq and Kamal Bansal, **Performance Evaluation of Energy Consumption in MANET** , International Journal of Computer Applications (0975 – 8887) Volume 42– No.2, March 2012, pp. 7-12.

4. M. Mohammed. **Energy Efficient Location Aided Routing Protocol for Wireless MANETs**, International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

5. O. Tariq, F. Greg and W. Murray. **On the Effect of Traffic Model to the Performance Evaluation of Multicast Protocols in MANET,** Proceedings Canadian Conference on Electrical and Computer Engineering, pp. 404–407, 2005.

6. B. Wang and S. K. S. Gupta. **On Maximizing Lifetime of Multicast Trees in Wireless Ad hoc Networks** , Proceedings of the IEEE International Conference on Parallel Processing, 2003.

7. R. Vaishampayan and J.J. Garcia-Luna-Aceves. **Energy Efficient and Robust Multicast Routing in Mobile Ad Hoc Networks**, Proceedings of the IEEE International Conference on Mobile Ad-hoc and Sensor Systems, 2004.

8. Y. Lia, X. Chengb and W. Wuc. **Optimal Topology Control for Balanced Energy Consumption in Wireless Networks,** J. Parallel and Distributed Computing, Vol. 65, No. 2, pp. 124 – 131, February 2005.

9. Cynthia Jayapal and Sumathi Vembu. **Adaptive Service Discovery Protocol for Mobile Ad Hoc Networks**, European Journal of Scientific Research ISSN 1450-216X Vol. .49, No.1 (2011), pp.6-17.

10. Yadu Kishore K, Ashish Tiwari and O G Kakde. **Optimization based Topology Control for Wireless Adhoc Networks to meet QoS requirements**, 2010 29th IEEE International Symposium on Reliable Distributed Systems, pp 30-36.