Efficient DoS Attacks Detection Technique in Mobile Ad-hoc Network

Anita Namdev
M.Tech Scholar,
Software Engineering,
LNCT , Bhopal (M.P.) India

Vineet Richhariya
Professor & HOD
CSE, LNCT
Bhopal (M.P.) India

Vivek Richhariya
Asstt. Professor
CSE, LNCT
Bhopal(M.P.) India

ABSTRACT

MANETs are dynamic peer-to-peer networks, which employ multi-hop information transfer without requiring an infrastructure. Due to their nature, they have unique security requirements. Traditional security mechanisms used in infrastructure networks may be inapplicable to MANETs. For example, the dynamic and transient nature of MANETs can result in constant changes in trust among nodes. MANETs suffers from not only the vulnerabilities as their infrastructure counterparts, but also peculiar threats and attacks (e.g., sleep deprivation, selfish misbehaving and Denial of Service (DoS) attacks) caused by unique characteristics of MANETs. Also, once a route is formed, any node in the route may turn malicious and may refrain from forwarding packets, modify them before forwarding or may even forward to an incorrect intermediate node. In this paper they proposed a flow based detection approach that uses novel detection features to identify the attacks in MANET. In our simulation, the results show that the secure is still efficient in discovering secure routes compared with normal model in MANET.

Keywords- MANET, Detection Scheme, DoS attacks.

1. Introduction

A MANET represents a infrastructure-less distributed system that comprises wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ad-hoc" network topologies, allowing people and devices to seamlessly internetwork with no pre-existing communication infrastructure and central administration. Comparably, infrastructure wired or wireless networks refer to networks that possess communication infrastructures (e.g., routers, gateways, base stations, and etc). All communication and control functionalities in such networks are through these infrastructures. The Internet and traditional cellular wireless networks are typical examples of infrastructure networks. Although many experimental packet radio networks were later developed, these wireless systems did not ever really take off in the consumer segment. When developing IEEE 802.11, the Institute of Electrical and Electronic Engineering (IEEE) replaced the term packet radio network with ad hoc network. [1].

AODV routing protocol provides control messages for route discovery and subsequent route maintenance but cannot guard against their flooding, deliberate dropping or malicious modification. Before a route is established, a malicious node can flood the network with false control packets, such as RREQs (Route Requests), congesting the network leading to DoS attacks. Once a route is formed, any intermediate node in the route, which turns malicious can drop packets, modify them be-fore forwarding or tunnel them. Our scheme is implement the prevention technique of DoS attack (Denial of services) addresses these malicious activities and detects the node, which is misbehaving both prior to route formation (during route discovery) and after its establishment (during communication). This scheme is reported to quantify the effectiveness of the proposed scheme; malicious activities were simulated in the mobile environment and the resulting performance analysis [2] and [4].

2. Background

2.1 Overview of DoS Attack Detection Approaches-

In the following, we overview detection approaches against the DoS attacks proposed both in the Internet context and MANET context, respectively.

2.2 DoS Attack Detection Types

Generally, the DoS attack detection approaches can be classified into two categories according to different detection methodologies (i.e. anomaly detection and misuse detection) they adopt. While approaches that exploit the misuse detection methodology are referred as DoS attack specific detection, approaches that exploit the anomaly detection methodology are called as DoS attack anomaly detection.

2.3 DoS attack specific detection

These classes of detection approaches usually focus on one specific DoS attack. By carefully observing a known attack, they extract its unique traffic features ahead of detection. A match between the pre-extracted features and the current traffic indicates the occurrence of such attack.

Disproportional packet rates: By investigating the DoS attacks that occurred in Feb. 2010, the authors discovered one unique feature of attack traffic: packets rates between two hosts or subnets are not proportional (i.e. packets are destined for a host or subnet from which too few packets are coming back). Based on this observation, they defined a measure $R(p)$: the ratio of forward packets with destination IP address prefix P to reverse packets with source IP address P. A significantly disproportional difference between the packets rates going to and from a host or subnet (i.e. high $R(p)$) strongly indicates of a DoS attack. The TCP SYN DoS attack and Smurf attack can be detected by this approach [3].

2.4 Disproportional control packets-

Experiment results of TCP SYN attacks on commercial platforms showed that, to shut down the victim server for 10 minutes, attackers need to inject at least a total of 300,000 SYN packets. During the same time period, however, the number of FINs (RSTs) remains largely unchanged. Therefore, there will be much more SYNs than FINs (RSTs) collected during the DoSperiod. The difference between the number of SYNs and FINs (RSTs) was defined as a detection feature, which was used to identify the occurrence of TCP SYN DoS attack.

2.5 Control packets ratio-

Similar to approach the authors defined the detection feature as the number of TCP, ICMP and UDP packets and their respective ratio in the entire control overhead. The TCP SYN DoS attack, UDP storm attack and ICMP Ping attack will result in a significant increase of this feature.

2.6 Flow intensity: The basic idea behind the detection approach proposed is similar to those approaches. The difference is that selected the traffic intensity of particular packet flow, e.g., TCP, ICMP and UDP as the detection feature. A significant rise of this feature indicates the DoS attack.

2.7 Ratio of new IP address: Investigation results in [6] showed that most source IP addresses are new to the victim during the DoS attacks, whereas most source IP addresses in normal network situations (i.e. no DoS attacks) appeared at the victim before. Motivated by this observation, in recent proposed to use the ratio of new IP addresses as the detection feature to detect the bandwidth DoS attack. This feature is homogeneous and stable in normal situation; while there will be a statistical change when the bandwidth DoS attack happens.

2.8 Complexity differential: Normally, an attacker performs a DoS attack using a large number of similar packets (in terms of their destination address, protocol type, execution pattern etc.) generated from various locations but intended for the same destination. Thus, there is a lot of similarity in traffic pattern. On the other hand, legitimate traffic flows tend to have many different traffic types. Hence, traffic flows are not highly correlated and appear to be random [6] and [7].

To measure the similarity, the complexity differential was defined-

The difference between the cumulative complexities of individual packets and the total complexity computed when those packets are concatenated to form a single packet. If the complexity differential of a packet flow is greater than a preset threshold, this flow is marked as DoS attack suspect.

2.9 DoS attack anomaly detection

Anomaly based detection first establishes *profiles* to characterize normal network traffic. These profiles are based on statistical features, such as traffic correlation, packet rate distribution and autocorrelation of flow packets. Traffic patterns that significantly deviate from these profiles are marked as intrusions.

SYN rate distribution through their experiments that the distribution of SYN packet rate of normal traffic can be modeled by the normal distribution. But the SYN packet rate distribution of DoS attack traffic was far from a normal distribution. The significant SYN rate deviation (exceeding a given threshold) indicates the occurrence of TCP SYN DoS attack.

In previous, discovered that there is a strong correlation between traffic patterns at the victim and at the attack source. Based on this observation, they proposed a proactive scheme to detect DDoS attacks using time series analysis. Like all anomaly detection approaches, this scheme built a profile for each selected DoS attack. For example, the number of ICMP ECHO packets is used to build a profile for the Ping Flood attacks. Any anomalies deviating from the predefined profiles are regarded as strong indications of a DoS attack.

Multiple features detection to detect DoS attacks more accurately and in a broader spectrum, multiple detection features are proposed to collaboratively identify a specific DoS attack. Many IP, UDP, and TCP based features, such as packet length and packet rate, are defined to build profiles of normal network traffic.

While these profiles are input into the neural network classifier for pattern classifications were used the support vector machines to analyze the input profiles.

Traffic Autocorrelation claimed that the attack traffic $y(t)$ experienced by DoS attack victims has unusually tremendous rate during the transition process of intrusion. Thus, DoS attacks have the characteristics that the frequency bandwidth of $y(t)$ is wider than $x(t)$, the normal traffic. In other words, the shape of autocorrelation of $y(t)$ tended sharper than the autocorrelation of $x(t)$. When the distance between autocorrelation of $y(t)$ and the autocorrelation of $x(t)$ exceeds a given threshold, the DoS attack is said to be detected [8].

2.10 DoS Attack Detection in MANET

As outlined in previous, extensive research on DoS attack detection has been carried out and large numbers of detection approaches have been proposed in the Internet. However, due to the unique characteristics of MANETs, these approaches cannot produce expected results in MANET. To achieve the detection of DoS attack in MANETs, some approaches have been proposed recently.

In recent, build their detection mechanism on the base of the Extended Finite State Automaton (EFSA) according to the specification of AODV routing protocol. They detect attacks, including DoS attacks, as deviations from normal conditions that are defined by EFSA. For defining the normal conditions, learning data are extracted beforehand from the same network environment where the test data are applied.

In order to detect the DoS attack and mitigate malicious control packet floods, previously proposed a statistics based detection scheme and a rate based control packet forwarding mechanism. In their design, each node maintains a count of RREQs received for each RREQ sender during a preset time period. At the end of the time period, the node computes some statistical measures: the rate at which it has been receiving route requests from each sender, average rate of RREQs per sender, deviation of all RREQ sources, and a cut-off rate threshold. One node whose RREQs rate is above the cut-off rate will be identified as DoS attacker and its RREQ packets will be dropped.

In Yi's work, a model of Ad Hoc DoS attack exploiting either control packets or data packets is presented. In addition, they introduce the neighbour suppression and path cut-off schemes to prevent this DoS attack. In their design each node sets up the processing priority and thresh-old for its neighbour node.

By setting a priority (the inverse proportion to node's frequency of originating RREQ) and a threshold (maximum of originating RREQ in a period time) for each neighbour node, one node decreases the sending node's priority and denies accepting its RREQ if the sending node's RREQ originating rate exceeds the threshold.
The DoS attack detection scheme proposed which was similarly built on the base of counting nodes' packet rate. In this scheme, each node maintains records of other nodes' packet (e.g., RREQ) rate during a preset time period. Once a node's packet rate exceeds a preset threshold (fixed or adaptive), this node will be identified as suspicious or malicious node and its packets will be suspended or dropped [2] and [9].

2.11 Open Issues of DoS Attack Detection in MANET

As present in many detection approaches have been proposed against the DoS attacks in both the Internet and MANETs. However, they are not able to detect the distributed DoS attacks in MANETs considered in this work. This type of attack exploits the broadcast transmission method used by many MANET protocols (e.g., routing protocols) to generate overwhelming traffic to paralyze the entire MANET. Here, we identify limitations of existing detection approaches in detecting the distributed DoS attacks.

2.12 Detection approaches in the Internet

The majority of detection approaches proposed in the Internet are designed to deal with DoS attacks at the transport layer. These transport layer specific detection approaches cannot be applied for detecting the distributed DoS attacks that exploit the network routing protocols in MANETs.
Besides those transport layer specific detection approaches, some generic detection mechanisms were also proposed, which can be applied in various protocols at different layers. However, assumptions on which these approaches are based do not hold in MANETs. For example, assumed that, during normal Internet situation, the traffic going through one direction is proportional to the traffic going through the opposite direction. If not, something must be abnormal. This assumption is not always true in the MANET environment where mobile nodes are constantly moving and network topology is frequently changing. This dynamic nature of MANETs makes it quite possible that the traffic from two reverse directions is not proportional.

2.13 Detection approaches in MANET

DoS attack detection approaches proposed were simply based on monitoring the nodes' packet rate. If one node's packet (RREQ) rate exceeds a given threshold, this node is considered as the attacker. These packet rate based detection mechanisms cannot detect the DoS attack performed by multiple colluding malicious nodes. This is because, by employing multiple accomplices, the attack traffic rate of each attack node can be normally low, but the aggregated attack traffic can be still huge enough to paralyze the network. Meanwhile, these rate based detection approaches could result in false positive detection when the flash crowd event happens.
Nodes transmit packets using real and valid addresses; they are unable to handle some DoS attacks where attackers spoof source addresses of attack packets with random ones [7] and [10].

3. Proposed DoS Attack Detection Technique

The basic idea behind detection approach is as follows. For a given statistical feature of the network traffic, it is stable and homogeneous in the normal network situation. However, the DoS attack can exclusively cause significant abnormality of this statistical feature. Detecting the DoS attack can be transferred to the identification of such abnormality. Hence, the task of detecting a DoS attack can for each DoS attack variation caused by different values of attack parameters, abstract a certain statistical feature of the network traffic. This statistical feature is stable and homogeneous in the normal network situation. When a certain DoS attack is launched, this feature will manifest significant abnormality, e.g., considerable increase or decrease. This abnormality is recorded as a *signature* representing the occurrence of such an attack. Monitor the ongoing network traffic and retrieve those statistical features abstracted in subtask. Seek a match between current behaviour of statistical feature and the recorded *signature*. We say the DoS attack is detected if such a match is confirmed.
In this paper we propose a detection feature, RREQ packet rate to detect high rate DoS attack.

3.1 Sequential Change Point Detection

As described before, RREQ traffic in MANETs is a complex stochastic process. The DoS attack can result in abrupt changes of certain RREQ traffic feature. Currently, two approaches are widely being used in the abrupt change detection:

3.1.1 Fixed-size batch detection and sequential change point detection.

The fixed-size batch detection is an on-line approach that first collects sampled data over a fixed time interval (one hour or one day). Then, it makes a decision of homogeneity or a change point. The sequential change point detection approach monitors and detects changes of detection variables on the run (on-line). Compared to the fixed-size batch detection approach, the sequential change point detection has advantages of quick detection and light requirements of memory and computation, which suit well the MANET environment. Thus, we decide to model the detection of DoS attack as a sequential change point problem.
Originally arising from statistical quality control, now the sequential change point detection has many other important applications, including reliability, signal detection, fault detection, surveillance, and finance and so on. Its objective is to determine if the observed variable series is statistically homogeneous, and if not, to find the point in time when the change happens. We, in this work, choose to apply the algorithm on random sequence $\rightarrow Xi$ to identify its changes.
The basic idea behind our method is as follows: if any change occurs on the observed statistical process, the probability distribution of such process will change correspondingly. We decide to adopt the non-parametric method to perform the change detection. The reasons are given as follows.
The parametric version of these algorithm requires a prior knowledge of statistical model for the random sequence $\{Xi\}$. However, due to the dynamic and complicated nature of MANETs, acquiring an accurate statistical model of the RREQ traffic still remains an open problem, which is beyond the scope of this thesis.

The non-parametric method, on the other hand, does not need such prior knowledge of statistical model. Instead, it monitors and records the mean value of the random sequence under a normal scenario. Then, it accumulates those values of random variables that are significantly higher than the mean value. Once these accumulated values exceed a given threshold, a change (or attack) is said to be detected.

To acquire these detection feature, each node counts the number of RREQ packets ($N_{i,j}$) belonging to a certain RREQ flow j seen in sampling interval Δti. At the end of Δt_i, this node can calculate the RREQ packet rate ($R_{i,j}$) of flow j, $R_{i,j} = N_{i,j} / \Delta t_i$. If this node *sees* k flows in Δti, the average RREQ packet rate, $avgRate_i$, of k *f*lows in Δt_i is calculated by Equation 1, and the standard deviation, $stdRate_i$, is given by Equation 2.

$$avgRatei = \sum_{j=1}^{k} Ri,j \Big/ k \quad \text{..... (1)}$$

$$stdRatei = \sqrt{\sum_{j=1}^{k} (Ri,j - avgRatei)^2} \Big/ k-1 \quad \text{..... (2)}$$

$$\mathbf{T_{Ratei}} = avgRate_i + 3.stdRate_i \quad \text{..... (3)}$$

The high rate DoS attack can be identified by the following rule: if a node's RREQ packet rate *Ri,j* counted in Δti exceeds a given threshold *TRatei* , this node is confirmed as a high rate DoS attacker at Δti. The adaptive detection threshold is given by equation 3.

We model the DoS attack detection as the sequential change point detection problem. Then, we propose to apply the non-parametric algorithm on our detection features to perform the DoS attack identification.

According to the non-parametric algorithm has a requirement for the applied random sequence $\{Xi\}$: the mean of $\{Xi\}$, α, is negative in normal scenario and becomes positive when a change (attack) takes place. To satisfy this requirement, we transform $\{Xi\}$ to $\{Zi\}$ by equation (4).

$$Zi = Xi - \beta \quad \text{.....} \quad (4)$$

where $\beta = \alpha + |a|$, and a is the mean of $\{Zi\}$. a is negative during normal conditions, and becomes positive when a change occurs. Then we de¯ne the third variable $\{Yi\}$ using equation (5)

$$Yi = (Yi\text{-}1 + Zi)^{+}, Y0 = 0 \quad \text{..... (5)}$$

where $X+$ is equal to X if $X > 0$, and 0 otherwise. From the definition of$\{Zi\}$, we can see that: (1) $\{Zi\}$ is negative in normal scenario; (2) When attack is launched, $\{Zi\}$ will become positive and large, i.e. $h + a > 0$. Thus, these positive values of $\{Zi\}$ are accumulated by $\{Yi\}$, and negative values are dropped. A large value of $\{Yi\}$ strongly indicates an attack. The decision function can be described as follows.

$d_T(Yi) = 0$; if Yi < T
$d_T(Yi) = 1$; if Yi >= T

T is the threshold for the attack detection and $d_T(Yi)$ represents the decision at time i. If Yi , T, $d_T(Yi)$ is `1', which indicates the detection of a change (attack). If $Yi$ is less than $T$, $d_T(Yi)$ is `0', meaning there is no change. The algorithm is summarized as follows:

input: Original values of detection feature $\{Xi\}$, T
Output: Detection decision $d_T(Yi)$
//
For each *Input* $\{Xi\}$ do
$Zi = Xi - \beta$;
$Yi = (Yi\text{-}1 + Zi)^{+}$;
if $Yi < T$ then
$dT(Yi) = 0$;
end
else
$dT(Yi) = 1$;
end
end
return $dT(Yi)$
//

We designed flow based detection features to characterize the DoS attack forms respectively.

We are able to handle all attack variations in the DoS attack spectrum. We modeled the detection of DoS attacks into the sequential change point detection problem, and proposed to apply the above algorithm on those detection features to identify the occurrence of DoS attacks in MANET.

3.2 Detection Performance Evaluation

We organize the evaluation procedure as follows. First, we examine the performance of detection features individually, i.e. Detection feature against the high rate DoS attack. For each detection feature, we evaluate its performance in terms of three metrics in different network environments. Then, we investigate the combination use of detection features. . By using them jointly, we expect that those DoS attack variations between the DoS attacks forms can be detected.

3.3 Evaluation Metrics

There are some properties of intrusion detection approach that are commonly expected: accurate and quick. First, attacks need to be detected as soon as possible. Accurate detection can be interpreted from two aspects. On one hand, people expect to detect all ongoing attacks. On the other hand, they want to minimize the possibility that non-malicious network scenarios are mistakenly judged as malicious scenarios, which is referred as false (positive) detection.

Therefore, we propose to use the following three metrics to evaluate our detection mechanisms.

***3.3.1 Detection Ratio* (DR, %)** -The ratio of the number of mobile nodes detecting attacks over the total number of nodes in the MANET. Since each and every node in the network independently perform the detection, this metric measures the accuracy of detection approach.

3.3.2 Detection Time (DT, second) -The interval between the moment when the attack is launched and the moment when it is detected. These metric measures how fast these detection approach works.

3.3.3 False Detection Rate (FDR, false positive detections per day). Our detection approach may have false positive detection. For example, some unusual (but not malicious) network activities, such as flash crowd event, may make our detection feature (DF) rise significantly. The increase of DF may be large enough to exceed the given threshold, trigger the detection alarm, and in turn lead to the false positive detection. In this work, they use DR and FDR to measure the accuracy property of our detection approach. Mainly based on simulation experiments, they tested how fast, how accurately and how economically our approach performs

the detection in terms of detection time, detection ratio and false detection rate. To validate the performance consistency of these detection approach, we simulated diverse network background scenarios and DoS attack scenarios, in which our detection approach was examined.

4. Results Analysis

DoS attack, its detection model and normal model all are executed in the same environment for comparison purposes in NS-2. The following choices are made for simulation considering accuracy of result and available resources. Then, we carry out quantitative and comprehensive evaluation of detection performance in terms of detection time, detection ratio, and false detection ratio and detection sensitivity. The simulation parameters of thesis work as follows:

Length of MANET	1000 to 1500 (M)
No. of mobile nodes	500
Packet rate of normal connection	1
Traffic type	CBR
Max. mode speed	5 m/s – 20 m/s
No. of connections between nodes	5 – 20
Pause time	20 s
Rate (packet per sec)	2 packets/s
Data payload (packet size)	28 – 512 bytes

Table: Simulation parameters

The packet rate of connections is chosen to avoid packet dropping caused by congestion even when there are multiple connections converting at the same host. The host moving speed converses a range from human jogging to vehicle riding in a country field. Faster speeds are not considered because the frequency of the route changes will be too high and the resulted performance degradation will not be entirely the effect of the active attacks.

We have performed number of simulations to show the effectiveness, usefulness and performance of routing protocols architecture. We have run number of simulations with variable nodes and communication flows in each simulation; a node may have send data to other node or act as an intermediate node. Average throughput, Packet delivery ratio and End to end delay are considered to evaluate the performance of the protocols.

4.1 Average Throughput

After several numbers of simulations they find out the average throughput for both the protocols while randomly changing the values of node density. In our secure model in MANET average throughput decreases from 580 to 482 when node number increases 0 to 30 after that average throughput increases from 482 to 483 when node number increases from 31 to 40, after then average throughput decreases from 483 to 433 when node number increases from 41 to 100 on the other hand average throughput decrease linearly with respect to increase the node number from 0 to 100 in non secure model (in figure 1).

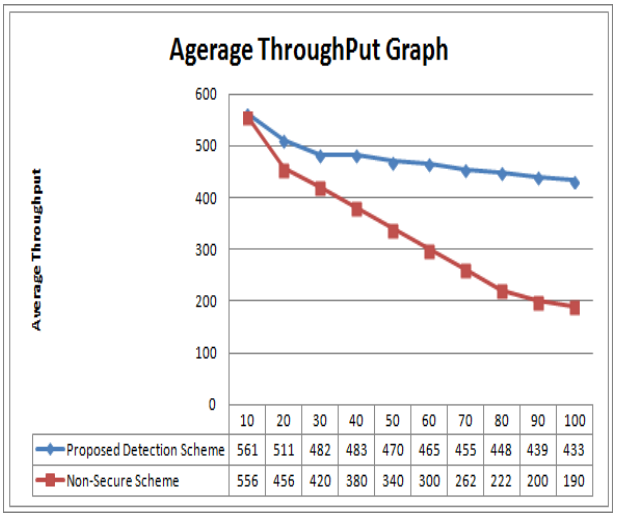

Figure1 Average Throughput vs. Number of Nodes

4.2 End to End Delay

In these secure model, end to end delay decreases from 833 to 810 and non-secure model end to end delay increases 833 to 866 when node number increases 0 to 30. After that in secure end to end delay decreases from 810 to 770 and normal end to end delay increases 866 to 890 when node number increases 40 to 60. Then secure end to end delay decreases from 770 to 740 and normal end to end delay increases 890 to 932 when node number increases 70 to 100 (in figure 2).

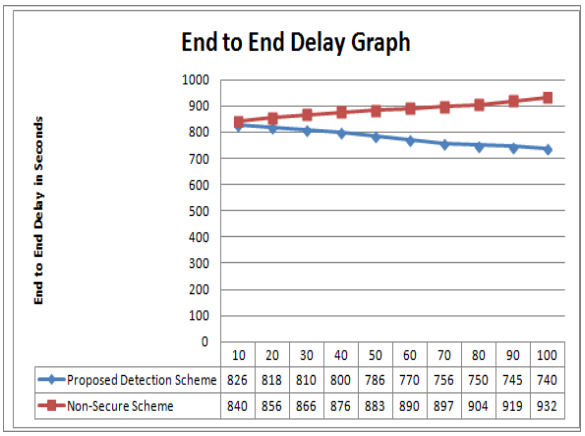

Figure 2 End to End Delay vs. Number of Nodes

5. Conclusion and Future Work

In this paper, they identified unique characteristics of MANETs that enable the execution of a DoS attack, which include broadcast, limited resources and “open" nature. Also, they described basic mechanisms behind the DoS attack, such as accomplices recruiting and address spoofing. Based on the above investigation, we modeled the DoS attack. In this model, they discussed what possible attributes this attack may possess, what the attack impact on the victim network is, and how these attributes diversify the attack patterns. The implementation of DoS attack and its Detection for wireless ad hoc networks provides real-time behavior with the use of

timed finite state machines. Although the idea of intrusion detection with the use of finite state machines has certain limitations but it resembles highly with real time behavior of ad-hoc networks. In future, the system could be also extended to include some cryptographic mechanism like a certification authority that would prevent nodes from impersonating other nodes.

6. References

[1] Wenchao Huang, Yan Xiong, Depin Chen, "DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation", IEEE 2009 International Conference on Computational Science and Engineering, Issue Date : 29-31 Aug. 2009, Volume : 2 , On page(s): 809 , Print ISBN: 978-1-4244-5334-4 INSPEC Accession Number: 10915441.

[2] A.H Azni, Azreen Azman, Madihah Mohd Saudi, AH Fauzi, DNF Awang Iskandar, "Analysis of Packets Abnormalities in Wireless Sensor Network" , IEEE 2009 Fifth International Conference on MEMS NANO, and Smart Systems, pp 259-264.

[3] Cuirong Wang, Shuxin Cai, "AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security", IEEE 2009 International Conference on Multimedia Information Networking and Security, pp 401-404.

[4] A Nagaraju and B.Eswar, "Performance of Dominating Sets in AODV Routing protocol for MANETs", IEEE 2009 First International Conference on Networks & Communications, pp 166-170.

[5] Sheng Cao and Yong Chen, "AN Intelligent MANet Routing Method MEC", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp 831-834.

[6] C. Ng, P. Thubert, M. Watari, and F. Zhao, "Network Mobility Route Optimization Problem Statement," RFC 4888, July 2007.

[7] Li-Li PAN, "Research and Simulation for Secure Routing Protocol Based on Ad Hoc Network", IEEE 2010 2nd International Conference on Education Technology and Computer (ICETC), pp 46-49.

[8] Liza Lai-Yee Shek and Yu-Kwong Kwok." Resource Management Schemes for Bluetooth Scatternets". International Conference on Parallel Processing Workshops (ICPPW'03), 2003 IEEE.

[9] Bin Zhen, Jonghun Park and Yongsuk Kim.," Scatternet Formation of bluetooth Ad-hoc Networks", Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03) 0-7695, 2002 IEEE.

[10] Sharifah Suhaila Mohd. Ramli, Halabi Hasbulla", Energy-Efficient Handover. Algorithm for Bluetooth Network", 2008 IEEE.