PROFIDES - Profile based Intrusion Detection Approach Using Traffic Behavior over Mobile Ad Hoc Network

R.Saminathan
Annamalai University
Annamalainagar – 608 002
Tamilnadu, India

Dr.K.Selvakumar
Annamalai University
Annamalainagar – 608 002
Tamilnadu, India

ABSTRACT

Intrusion Detection in MANET is one of the major concern in peer-to-peer networking scenario where mobile / wireless nodes communicate with each other without any pre-defined infra-structural setup. This paper presents an overview of various intrusion detection models, identifying its issues, discusses on design and proposes an intrusion detection system using profile based traffic behavior scenario (PROFIDES), to determine misbehaving nodes by generating alerts based on critical parameters to identify an intrusion activity. The proposed system had been checked primarily for Packet Drop attacks, where the performance is effective over AODV and its other counterpart protocols. PROFIDES works in highly dynamic varying environments where any variation in traffic intensity of MANET is analyzed to adapt for different traffic behavioral patterns.

Keywords

Intrusion Detection System, Misbehavior, Traffic Intensity, Threshold value, Packet drop.

1. INTRODUCTION

The major task of intrusion detection system [1] is to discover the intruders from the network packet traffic data or system audit data. In an ad hoc network, malicious nodes may enter or leave the immediate radio transmission range at random intervals or may collide with other malicious nodes to disrupt network activity or behave maliciously only intermittently, further complicating their detection. A node that sends out false routing information could be a compromised node, or merely a node that has a temporarily stale routing table due to volatile physical conditions. Packets may be dropped due to network congestion or because a malicious node is not faithfully executing a routing algorithm.

MANET [6] is defined to be a collection of mobile / wireless nodes adopting a peer to peer communication with each other. Research efforts [2], [3], [4] work consistently to provide efficient / reliable and secured communication between nodes in a network.

MANET does not have any concentration points where IDS can collect audit data for the entire traffic monitoring process in network [12]. The wireless links between nodes are highly susceptible to link attacks, which include passive eavesdropping, active interfering, leakage of secret information, data tampering, impersonation, message replay, message distortion, and denial of service. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks [3], [4] might allow the adversary to delete messages, inject erroneous messages, modify messages, and impersonate a node, thus violating availability, integrity, authentication, and non repudiation. Every node in the ad-hoc network must be prepared for encounter with the adversary.

In this paper, we propose an IDS system termed PROFIDES which monitors the behavior of MANET network, identifies the type of traffic generated and generates alert mechanism when the system tries to cross the defined threshold limit ‘T’. This limitation factor ‘T’ tries to improve the degradation behavior of system and brings the system back into normality.

The objective is to present a simple IDS architecture based on node behavior and profile which can work on AODV routing protocol [6]. The design focuses on the mobility and autonomy associated with mobile nodes to provide an efficient and flexible solution to security issues for session connectivity between nodes.

The proposed work PROFIDES performs well against various attacks [13], [15] which is discussed in Section 5. The rest of the paper is as follows: Section 2 elaborates on survey of literature review which reveals the need for PROFIDES. Section 3 discusses on the architecture, design prospective of PROFIDES. Section 4 elaborates on the functionality and modeling approaches, while Section 5 discusses on the experimental methods adopted to test the proposed setup. Section 6 discusses on results and future work to be done.

2. LITERATURE SURVEY

Zang and Lee [14] describe a distributed and collaborative anomaly detection-based IDS for ad hoc networks. Sergio Marti et al [7] describe an approach that involves the use of finite state machines for specifying correct AODV routing behavior and distributed network monitors for detecting run-time violation of the specifications. Yi and Naldurg [13] present a method for building confidence measures of route trustworthiness without a central trust authority. Papadimitratos [5] and Z. J. Haas [16] present various passive methods for establishing trust metrics and evaluating trust during run time.

Michiardi and Molva [3] assign a value to the “reputation” of a node and use this information to identify misbehaving nodes and cooperate only with nodes with trusted reputations. E. Z. Ang [1] couple a trust-based mechanism with a mobile agent based intrusion detection system, but do not discuss the security implications or overhead needed to secure the network and individual nodes from the mobile agents themselves. Sun, Wu and Pooch [9] introduce a geographic zone-based intrusion detection framework that uses location-aware zone gateway nodes to collect and aggregate alerts from intra-zone nodes. Gateway nodes in neighboring zones can then further collaborate to perform intrusion detection tasks in a wider area and to attempt to reduce false positive alarms.

Sterne [8] proposed a generic architecture of IDS which tries to improve throughput in MANET in the presence of nodes that agree to forward packets but fail to do so. In MANET, cooperation is very important to support the basic functions of the network so the token-based mechanism, the credit-based mechanism, and the reputation-based mechanism were developed to enforce cooperation.

Tseng [11] proposed “intrusion detection (ID) and response system” should follow both the natures. In this proposed architecture model, each node is responsible for detecting signs of intrusion locally and independently, but neighboring nodes can collaboratively investigate in a broader range.

3. PROFIDES – APPROACH

A profile based neighbor monitoring mechanism has been used to detect the abnormal behavior in the system. The basic routing mechanism is AODV [1]. It is a reactive routing protocol which creates route only when required. The work is organized into various phases such as data collection, feature selection, Profile based Intrusion Detection System (PROFIDES). The data collection phase collects the audit data from the various sources. The feature selection phase collects the features from the raw data. The intrusion detection phase detects the intrusion activity based on the traffic intensity at any instance within the communication system.

PROFIDES predicts on the assumption that intrusion attempts can be characterized by sequences of user activities that lead to uncompromised system states. PROFIDES is characterized by its properties which issues policies when audit records or system status information begin to indicate an illegal activity. The predefined policies typically consider high-level state change patterns observed in the audit data or collected data compared to predefined penetration state change scenarios. If the profile system infers that a penetration is in process or has occurred, it will alert the system security modules and provide them with both a justification for the alert and identification of the suspected intruder.

3.1 System Architecture

The anomaly detection method identifies intrusive activities as being a sub-set which cannot fit into normal activity patterns. The PROFIDES system architecture, shown in Figure 1, will have a set of modules which try to quantify normal or acceptable behavior of a user, storing it in user profiles thus monitoring and identifying irregular behaviors of user as intrusion. However, the system has an Event Handler Module that look for attacks that can be precisely identified by the way they occur, such as intrusions that follow a well-defined pattern of attack (attack signatures), and these are characteristics of the model of improper usage detection (abuse).

The proposed architecture represents itself as a hybrid between the anomaly detection model and misuse detection model. This can also be considered a significant advantage, since monolithic hybrid systems are complex, implying severe performance penalties on the environment to be monitored, which is not the case with the modular proposal.

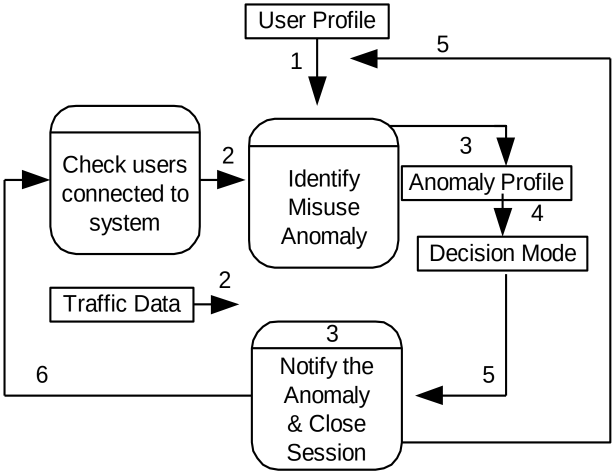

Figure 1 Modeling of Anomalous User Identification

In terms of data treatment, the architecture is a hybrid of a host-based model and a network-based model. The characteristics of a host-based system include a set of agents that look for deviations from standard behavior based on the profiles of usage of a piece of equipment, using statistical models or specialized systems. The hybrid nature of the proposed architecture allows it to make use of the advantages of each classification methodology, contributing to the development of a robust and efficient intrusion detection system.

3.2 Design

Design of PROFIDES can be discussed in four steps:

[a] Assigning a preset profile for the nodes involved in communication in mobile – ad hoc setup.

[b] Gathering Traffic intensity of nodes between the source to destination and adopting an analysis procedure.

[c] Identifying the anomaly or misuse node based on monitoring and analysis of its behavior.

[d] Isolating the intruder node from its normal activity and update it to “Intrusion Profile”.

PROFIDES adopts an effective indexed profile based mining approach [2] to detect intrusion in MANET communication networks. The system performs consistent check on intrusion detection activity by monitoring the behavior of source node’s neighbors. The network traffic is captured, if intensity is abnormal, monitored and preprocessed for all types of data packets. In the data preprocessing analysis [10], each node will monitor its neighbors’ traffic and select the features from the available traffic data required for attack analysis. According to these features, each node builds a profile on it, which monitors all the possible / available traffic features. Once the traffic feature exceeds the threshold ‘T’ (defined as in Section 4) an alert is generated. Since anomaly detection is focused in this research work, identification of abnormal data is considered as “intrusion profile”, as well any deviation from the normal activity is considered as anomaly.

4. MODELING THE SCENARIO

The working structure and functionality of PROFIDES scheme is shown in Figure 2.

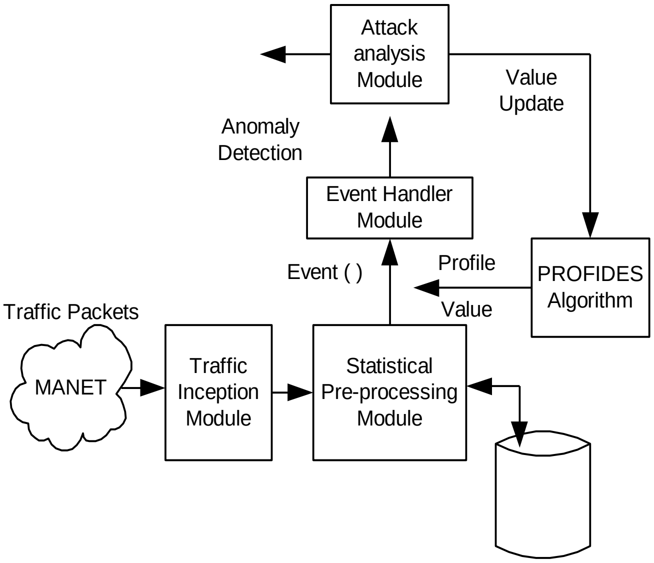

Figure 2 Working Structure and Functionality of PROFIDES Scheme

[a] Traffic Inception: This phase collects the incoming traffic data from the network system and classifies based on type of packets (data packet, route control packet, signaling packets) which are to be processed. The control packet includes route request route reply, or route error packets of AODV. It is necessary for an intrusion detection system to collect the data in a reliable and efficient manner.

[b] Statistical Preprocessing: Statistical Preprocessing module is responsible for feature selection. The traffic feature can be either a

data specific or route specific, or flow direction which can take any of the following values such as number of packets received, sent, forwarded or dropped. The preprocessor will keep the count of packets transacted for each sampling interval.

[c] Threshold generation: This module checks consistently the abnormal behavior of nodes in network. Any unexpected change in normal behavior of the system is termed as 'abnormal' and taken into monitoring. Each node maintains the profile for its neighbors. These profiles contain traffic related features monitoring the node's behavior, if the traffic feature exceeds the threshold, then anomaly is detected. The Threshold Value 'T' is vector in quantity, hence dynamically assigned based on traffic flow and number of users connected to system.

[d] Event generation Module: This module is responsible for collecting the essential information required for the attack analysis which determines whether there is any malicious activity in the network using PROFIDES algorithm.

[e]Intrusion detection system mechanism: This module makes use of anomaly detection method in which a baseline profile of normal activities are created. Any system activity that deviates from the baseline is treated as possible intrusion. In this architecture each node builds a profile for each of its neighbor. The profile includes the traffic features such as packet type, and flow direction. Once the traffic feature exceeds certain threshold an alert should be produced. The profile based neighbor monitoring algorithm makes use of mean and standard deviation model to detect the anomaly. The PROFIDES operates between the network traffic and the routing protocol.

[f] Traffic Profile: The process of identifying an anomaly pattern in a dataset D can be regarded as the average probability of observing a similar pattern from a node to node transaction in MANET setup. It can be understood from the following definition.

If M be the profile over a set of traffic pattern intensity {δ1, δ2, . . . , δn}. The estimated support of δk is written as $\hat{s}$ (δk),

$$\hat{s}(\alpha_k) = \mathrm{s}\,(\mathrm{M}) \prod_{\mathrm{o}_t \in \alpha_k} p\,(x_i = 1)$$

Where s(M) = $\dfrac{|\,\mathrm{D}_{x1} \cup \ldots \cup \mathrm{D}_{x2}\,|}{|\,\mathrm{D}\,|}$

p is the distribution vector of M,

Xi is the boolean random variable indicating the selection of item δi in pattern δk.

while, D being the dataset of traffic patterns.

It is noticed that calculation of an estimated support is only involved with d + 1 real values, where d-dimensional distribution vector of a profile and the number of transactions that support the profile is considered. This result becomes one of the most distinguishing features in our summarization model. Hence, it can be understood that we can use much limited information in a data packet profile to identify or recover the support of a rather large set of traffic similar patterns.

[g] Anomaly Intrusion Pattern Mining Process: Given a set of traffic patterns M = {α1, α2, . . . , αm} that are mined from a traffic dataset D = {t1, t2, . . . , tn}, pattern summarization is to find K pattern profiles based on the pattern set M.

A potential solution to the summarization problem is to group frequent anomaly packet patterns into several clusters such that the similarity within clusters is maximized and the similarity between clusters is minimized. Once the clustering or similar grouping is done, the profile set for each cluster can be calculated.

We can construct a specific profile for each pattern that only contains the similar anomaly pattern itself. Using this representation, we can measure the distance between two patterns based on the divergence between their profiles. The distance between two patterns should reflect the correlation between the transactions that support these two patterns. Namely, if two patterns α and β are correlated, Dα and Dβ likely have large overlap; and the non-overlapping parts exhibit high similarity. Several measures are available to fulfill this requirement.

[h] Alert generation: If a node detects an intrusion with high evidence, it can initiate a response. If the node detects the intruder, an alert should be produced as Message or Alarm of few decibels such that user gets informed.

5. MANET TEST-BED ENVIRONMENT CREATION / DATA COLLECTION

A mobile ad hoc environment should be created by setting the required parameters. The data collection module is responsible for collecting the audit data from various sources. It is not possible to collect all the information for intrusion detection system. So, raw data should be passed to the preprocessing module to detect anomaly. This module collects the data through network packets. It can be a data packet or route specific packet.

The simulation of the proposed procedure can be carried out as follows:

1. MANET test-bed environment setup and data collection
2. Preparing Profile Feature selection
3. Profile Based Intrusion detection System Mechanism (PROFIDES)
4. Performance Evaluation and Enhancement

5.1 Mined-Feature Selection

Raw data is monitored for a specific time interval and the features are collected. The traffic feature can be packet type and flow direction. The control traffic includes the RREQ, RREP, RERR packets of AODV and HELLO packets. It keeps the count of packets transacted for each sampling interval.

Table 1 PROFIDES Feature values

Dimension	Values
Packet type	Data, Route (all), Route Request(RREQ), Route Reply(RREP), Route Error(RERR) and HELLO message
Flow Direction	Received, Sent, Forwarded and Dropped
Statistics Measure	Count the average and standard deviation of number of packets or size of data packets

5.2 The Profile Based Intrusion Detection System Mechanism

Each node monitors its neighbor traffic and builds a profile for each of its neighbors. The profile includes all the features as shown in Table 1. This profile is used as a threshold to detect intrusion. Mean and standard deviation are calculated for each sample of data. The set of upper and lower bound values for the anomaly has to be prepared. Once the traffic feature exceeds the threshold, an alert should be produced. The node can use the profile to monitor the neighboring node's behavior as shown in Figure 3.

Any statistical modeling approach could be used to analyze the behavior, where for any random traffic packet of value *x* gathered from *n* observations of user A, the statistical model determines whether the next new traffic packet observed from the user B as observation x_n+1 is abnormal with respect to the previous observations. A new observation x_n+1 is abnormal if it falls outside a behavioral interval defined.

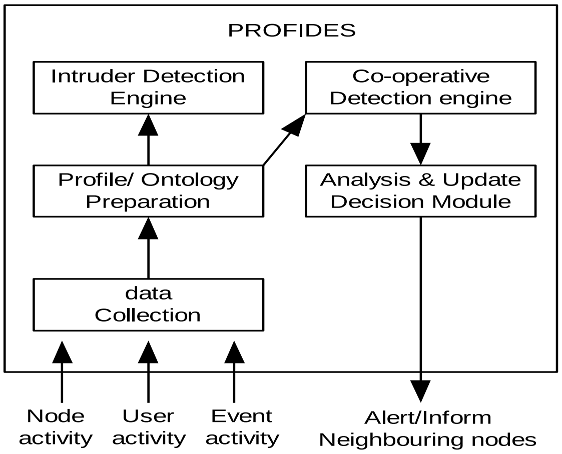
PROFIDES
Intruder Detection Engine
Co-operative Detection engine
Profile/ Ontology Preparation
Analysis & Update Decision Module
data Collection
Node activity
User activity
Event activity
Alert/Inform Neighbouring nodes

Figure 3 Profile Based Intrusion Detection Process

The algorithm for the PROFIDES scheme uses ns-2 [4] as shown in Figure 4, while maintaining the profile log record as shown in Figure 5.

```
Data : X : f1,f2,…. fn //percentage of traffic indentified at nodes
       Y : y1, y2,.. yn // number of packets dropped
       Z : z1, z2,.. zn // percentage of unknown packets identified
       T : Threshold value set

Result : Pv : AnomalyDetect (-1)
              Normal (0)
              UnknownDetect (1)
Begin :
(1)   OnEvent (X) AND {If Avg(Z) OR OnEvent(Z)}
(2)    If [Event(X) > T] AND
      {If Avg (Z) > Avg (Event(X) ) OR [Event (Y) > T] }
        Then  Pv = AnomalyDetect
       Else  Pv = Normal

(3)    If [ Event (Y) > T] AND
      {If Avg (Z) > Avg (Event(Y)) OR [Event (Y) > T] }
        Then  Pv = AnomalyDetect
       Else
          Pv = Normal

(4)    If [ Event (Z) > T] AND
      {If Avg (Z) > Avg (Event(Y)) OR [Event (X)] }
        Then  Pv = UnknownDetect
       Else
          Pv = Normal
End.
```

Figure 4 PROFIDES Event-Threshold Algorithm

```
class PROFIDES {
  public:
     void recvPacket *p, Handler *t;
     int command (int, const char *r),target_profile;
     int initialized ( ) {
       return target_profile;
      }
   private:
        AttackTimer a_timer;
       /* attack information */
       nsaddr_1 a_target;
       int a_type; /* attack type */
       double a_interval;
       void send_AttackRequest();
       void start_Attack();
       void stop_Attack();
       void attack_Timeout(int);
};
```

Figure 4a PROFIDES: Profile and Log Record Definition

5.3 Performance Evaluation and Enhancement

The architecture is examined and performance evaluation for traffic intensity, packet drop, number of attacks occurred is shown by plotting graphs. AODV based IDS performance has been compared and evaluated with same attack scenarios [Figure 4b] with the proposed system.

5.4 ns-2 Simulation scenarios for PROFIDES

The tests performed are representative of the overall results. The test bed simulated using Network Simulator ns-2 [12] uses the following common parameter settings:

- Commands in each user record: 100 records
- Training sample size: 1875 records (75% of available records)
- Legitimate user test sample size: 625 records (25% of available records)
- Anomaly records created: 200

In order to construct the anomaly detection model for MANET routing, the experiment was conducted using ns-2. Table 2 shows the simulation parameters required to evaluate the PROFIDES algorithm Figure 4a.

Table 2 Simulation Parameters in ns2

Parameter	Value
Simulation Duration	100 s
Simulation Area	800 x 800
Number of Nodes	50 / 90
Transmission Range	250 m
Node Movement Model	Random Way Point
Packet Type	CBR (UDP)
Data Payload	512 Bytes
Maximum Speed	1 – 25 m/s
Routing Protocol	AODV, DSR,TORA,DSDV PROFIDES over AODV
Interface Queue Type	Drop Tail

A simulation of mobile ad hoc environment has been created using 50 nodes with embedded parameters mentioned in Table 2. The simulation time lasts for 100s. The random way point model in ns-2 is used to emulate node mobility pattern with a topology of 800x800m. The effectiveness of the architecture is compared to the existing approaches with the help of different graphs.

A node movement scenario consisting of 50 nodes moves with a minimum movement speed of 1 m/s and maximum movement speed of 25 m/s is created. The average pause between the movements is assumed as 1s and the simulation ends after 10s. The topology boundary is defined as 800x 800.

5.5 Attack implementation

The black hole attack and packet dropping are implemented to model the PROFIDES in MANET.

[a]Black hole attack: All the traffic is redirected to a specific node which may not have any traffic at all. A malicious node broadcasts a route request message with a selected source node and destination and a fake maximum sequence number.

In the route request packet, the malicious node claims a one-hop distance to the source node. The fake route request is then flooded in the network as it has the highest sequence number. All the nodes that receive the route request packet will update their route table with a reverse path to the victim through the malicious node. If the malicious node sends several route request messages with different source nodes, eventually it attracts most of the traffic in the network.

[b]Packet dropping attack: It simply drops the packets or route packets whenever it feels necessary.

// start blackhole or drop packet attack

```
void AODV::startAttack()
{
     attacking_ = 1;
     fprintf(stdout, "set attacking_ : %dn", attacking_);
     attacktimer.resched(0.);
}
 void AODV::stopAttack()
{
    attacking_ = 0;
    attacktimer.cancel();
}
void AODV::attackTimeout(int interval)
{
   if (attacking_)
        fprintf(stdout, "attackTimeout, send route request");
   sendAttackRequest();
   attacktimer.resched(1);
}
```

Figure 4b PROFIDES: Attack Functionality

6. RESULTS AND DISCUSSION

To evaluate the PROFIDES system, the metrics such as Traffic Intensity, Mobility Rate, Packet Dropping, and Number of Attacks Identified are considered. The traffic intensity is defined as:

*Traffic Intensity = (No. of Packets Received / No. of Packets Sent) *100*

The metrics are used to measure the severity of different types of attack. The mobility factor is defined as the rate at which the nodes are moving from source to destination. Since each node can monitor its neighbor's behavior, the system can detect whether a node has forwarded a routing packet or not. Packet drop is found to increase, when the node mobility rate increases. As the node mobility increases the participating nodes can initiate the route discovery process and the malicious node can drop more attacks. When compared to the AODV based IDS [13], PROFIDES activity over AODV is found to detect the attack earlier in time.

The simulation experiment was carried out for each profiled user in the IDS, while the false alarm rate for each user was determined using training patterns and test sequences (final partition of the data set) Figure 4b. The detection rate was obtained by using their training patterns and the test sequences from all the remaining users. The use of a smaller cluster size is preferable for increasing inter-user variability (improved detection rate), assuming that the quality of characterization is high. PROFIDES effort to minimize the false alarm rate has resulted in 85% of the 20 users having a false alarm rate of 20% or less. It was noticed that, only 35% of the users had an alarming intrusion detection rate of 80% or more due to the inadequacy in characterization. An option for increasing the detection rate without further increasing the false alarms is to observe the mobility sequences, from the traffic parameter dataset, which was missing in the training set.

The experimental test-bed for anomaly detection approach works in a predictable end for mobile ad-hoc networks. The normal behavior of a routing protocol can be established and used to detect anomalies for which standard MANET protocol such as AODV was chosen as the subject of study. One important parameter noticed is that the 'node mobility pattern' has high impact on identifying misbehavior performance. The performance was measured with the 'random way point mobility model'. The simulation area spanned a square of 800x800m in which 50 / 90 nodes move around, while all the parameters required for implementation were set for 100 nodes. The mobility pattern and traffic patterns were generated successfully so that nodes can transmit packets along with beacon signaling. The malicious nodes were introduced in the network by introducing packet dropping and black hole attack.

The increase in traffic intensity and abnormal packet dropping has high impact on performance of system. Besides the examined aspects, other parameters are also relevant for the performance of PROFIDES. The detection accuracy of PROFIDES is on an average of 72 % when compared with the results of AODV Figure 5. The performance was evaluated based on metrics such as (a) Attack Identification Rate, (b) Packet Drop Rate (c) Traffic Intensity between nodes (d) Mobility Ratio Figures 5, 6, 7, 8.

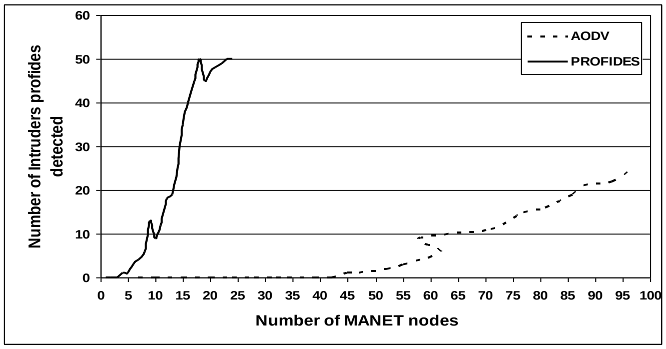

Figure 5 Attack and Intrusion detection rate

As time increases, any increase in Traffic Intensity leads to packet drop which confirms Figure 6, the policy that malicious nodes would be continuously dropping packets at certain intervals of time.

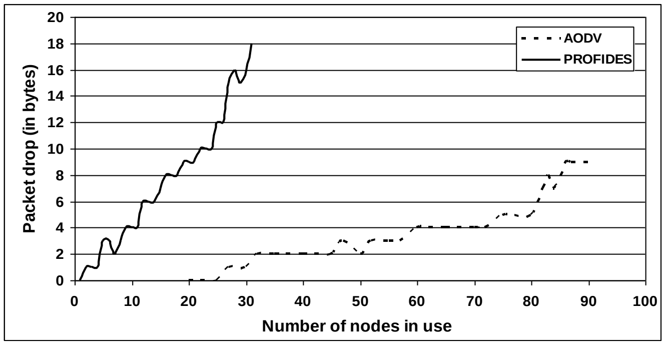

Figure 6 Packet drop rate

Figure 7 shows the network with intruder malicious node being detected, where intrusion detection activity for PROFIDES was 30 msecs to 50 msecs earlier compared to AODV. The intrusion detection process carried out PROFIDES was beneficial since it detects earlier in time, as well updates to User Profile Figure 2, which isolated such nodes from normal activity.

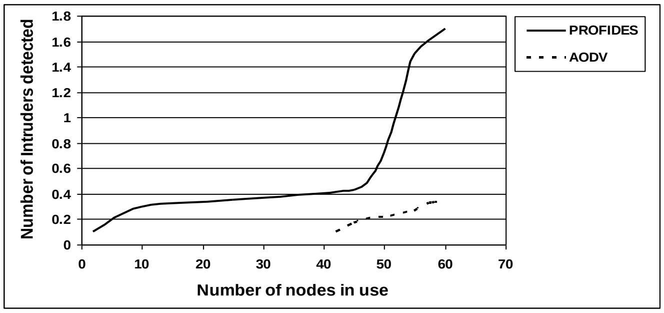

Figure 7 Intrusion Detection

The traffic intensity increases with time, as shown in the Figure 8. Traffic intensity increase may also be due to node mobility as known, since when time increases the node mobility increases. As node mobility increases it could be understood that the participating nodes can initiate route discovery process and malicious nodes can drop more packets disturbing the network connectivity.

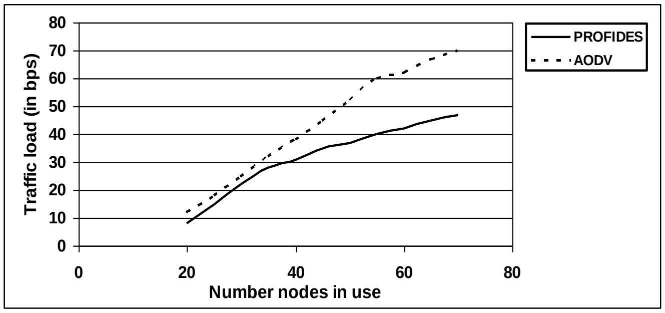

Figure 8 Traffic Intensity

To evaluate the attack identification rate, the number of attackers identified Figure 5 and time metrics Figure 6 are considered. When compared with the AODV protocol, it was identified that PROFIDES detection rate is better, while detection is faster. Figure 8 shows the performance of PROFIDES over AODV protocol, where packet drop is increased on increase of traffic load due to mobility of nodes.

7. CONCLUSION & FUTURE WORK

This paper presents a simple mechanism of intrusion detection or misbehaving nodes using profile based mining approach PROFIDES. Even though research works had been carried out in IDS, the need for intrusion activity based adaptive system was found void, since any change in system behavior or varying traffic intensity is always a misnomer. PROFIDES works in highly dynamic varying environments where, traffic intensity increases on mobility or increase in nodal activity. PROFIDES also controls the traffic intensity in setup as time increases by duly informing all other nodes about the attacker.

Such critical performance metrics improve the effectiveness and reliability with security in MANET. Future work can be carried out by introducing fuzzy set which can improve the process of identifying intruders being anomaly or misuse. The work can also focus on research plans to work on identifying multi-path security for large number of varying node intensity.

7.1 Acknowledgement

The authors wish to acknowledge the team of “Net Research Labs”, for providing suggestions in conduct of experiments as part of their research work.

REFERENCES

[1] Ang, E. Z. "Node Misbehaviour in Mobile Ad Hoc Networks," National University of Singapore, 2004.

[2] Gionis , Afrati, H. Mannila. Approximating a collection of frequent sets. In Proc. of 2004 ACM Int. Conf. on Knowledge Discovery in Databases (KDD’04), pg 12 – 19, 2004.

[3] Michiardi.P and R. Molva, “CORE: A Collaborative Reputation mechanism to Enforce node cooperation in mobile ad hoc networks,” Communication and Multimedia Security Conference (CMS'02), September 2002.

[4] NS2 network simulator. http://www.isi.edu/nsnam/ns.

[5] Papadimitratos.P, Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks", In Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January. 2002.

[6] Perkins C.E, E.M. Royer, S.R. Das, “Ad hoc On-Demand Distance Vector Routing” draftietf-manet-aodv-08.txt, IETF MANET Working Group, June 1st, 2001.

[7] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, Proc. 6th annual International Conference on Mobile computing and Networking, U.S.A, 2006.

[8] Sterne.D, P. Balasubramanyam, et al. “A General Cooperative Intrusion Detection Architecture for MANETs”, Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, 2005

[9] Sun.B, Wu, U.W. Pooch, “Zone-based intrusion detection for mobile ad hoc”, International Journal of Ad Hoc & Sensor Wireless Networks, September 2004.

[10] Tung. A, J. Pei, Han, Fault-tolerant frequent pattern mining: Problems and challenges. In Proc. of 2001 ACM Int. Workshop Data Mining and Knowledge Discovery (DMKD’01), pages 7–12, 2001.

[11] Tseng, P et al, A specification based intrusion detection system for AODV, Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 125–134. ACM Press, 2003

[12] Xiao et al, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, Wireless/Mobile Network Security, pg 131-169, Vol No 6,2006

[13] Yi.S, P. Naldurg and R. Kravets, Security-Aware Ad-Hoc Routing for Wireless Networks, UIUCDCS-R-2001-2241 Technical Report, 2001

[14] Zhang.Y, W. Lee, and Y. Huang, “Intrusion detection techniques for mobile wireless networks,” Wireless Networks Journal (ACM WINET), vol. 9, no. 5, pp. 545-556, September 2003

[15] Zhang.Y, and W. Lee, “Intrusion detection in wireless ad-hoc networks,” in Proc. 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, 2000, pp. 275–283.

[16] Zhou.L and Z.J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no. 6, Nov./Dec. 1999.