TRUST BASED SECURITY MECHANISM FOR SERVICE DISCOVERY IN MANET

S.PARISELVAM[1] AND R.M.S PARVATHI[2]

[1]Research scholar, Anna University.
Associate Professor, Manakula Vinayagar Institute of Technology, Pondicherry
[2]Principal and Professor, Department of Computer science and
Engineering, Sengunthar Engineering College, Tamilnadu, India
E-mail: [1]pariselvamphd@gmail.com

ABSTRACT

Mobile AdHoc Network (MANET) endures wide number of security issues in discovering services. Furthermore, different services require different level of security. For instance commercial applications necessitate less security compare to military applications. Thus, evolving an efficient service discovery mechanism in view of above criteria is a complicated work. In this paper, a trust based security mechanism for service discovery in MANET is proposed. This mechanism computes confidence or trust value for each node considering its interaction and behavior in the network. The trust model designates different protection level for services. Based on this protection level of the services, secure communication is offered. Further, the secure communication channel is established among nodes by sharing secret keys. By simulation results, we show that the proposed mechanism provide better security against attacks with reduced packet drops.

Keywords: *MANET*, *Trust*, *Security Mechanism*, *Service Discovery*

1. INTRODUCTION

1.1 Mobile Adhoc Networks (MANETs)

Mobile ad hoc networks (MANETs) consist of wireless mobile nodes without reliance on fixed base stations or wired infrastructures. This infrastructureless nature of MANETs poses an extreme challenge for the design of conventional and Quality of Service (QoS) routing protocols. [1] There is no fixed topology due to the node mobility, which results in interference, multipath propagation and path loss. Mobile nodes are restricted in battery power, computation capacity, bandwidth, and wireless channel leading to number of challenges while designing routing procedures. [2] While a mobile node can communicate directly with the nodes lying within its transmission range, communication with the mobile nodes outside of the transmission range must necessarily be multi-hop and require the establishment of communication paths. [3]

1.2 Service Discovery in MANET

Service discovery, which allows devices to advertise their own services to the rest of the network and to automatically locate network services with requested attributes, is a major component of MANETs. In the context of service discovery, service is any hardware or software feature that can be utilized or benefited by any node; Service description is the information that describes a service's characteristics, such as its types and attributes, access method, etc.; [4]

A server is a node that provides some services; A client is a node that requests services provided by other nodes. When a node needs services from others, it generates a service request packet. When receiving the request packet, each node that provides matched services responds with a service reply packet. Nodes without matched services forward the packet further. All these packet transmissions, including request packets and reply packets, form a Service Discovery Protocol (SDP) session. The objective of service discovery protocol is to reduce service request packet redundancy while retaining service discoverability. [4]

Discovery protocols enable software components to find each other on a network, and to determine if discovered components match their requirements. Further, discovery protocols include techniques to detect changes in component availability, and to maintain, within some time bounds, a consistent view of components in a network. [5]

However, in the context of MANETs, the following new challenges arise: Node mobility, affecting service availability frequent disconnections of the server or the client or intermediate nodes breaking or changing the path and the service selection parameters Channel variability, leading to significant communication characteristics variability (data rate, delay, etc.) [6]

According to their threat model, nodes can be categorized as: failed (nodes/victims of attacks), selfish (participating in the service discovery process only when it is convenient for them), and malicious (nodes trying to disrupt the service discovery process). [6]

1.3 Security Requirements for Service Discovery Mechanism

A security requirements model specific to service-oriented architectures was clearly defined. According to this model, there are four sets of security requirements regarding:

- **Service registration and deregistration:** during this phase, mutual authentication between directories and providers must be ensured. Also, upon service registration, service integrity must be kept until deregistration from the directory.
- **Service discovery**: only authorized clients must be allowed to discover services and only those services for which they have access rights. Moreover, service requests and replies must be kept confidential so that an attacker/eavesdropper cannot perform an inventory of available services and devices.
- **Service delivery**: during delivery, the service must be protected against malicious tampering or accidental modifications by intermediaries.
- **Service availability**: the system must be able to handle denial of service attacks, including denying service discovery to illegitimate clients. [6]

1.4 Security Issues of Service Discovery

- The model for dynamic service providers are failed if a single malicious node inserts into the network. So there must be security for preventing malicious node to get inside the network [7].
- The nature of ad hoc networks poses a great challenge to system security designers; the lack of Trusted Third Party adds the difficulty to deploy security mechanisms [7].
- Many challenges remain to be resolved before SDPs for multihop manets can be practical, for example, determining which type of overlay suits manet environments under high mobility. [8]
- In MANET, there is no need for an adversary to get the physical access to visit the network. Once the adversary is in the radio range of any other nodes, it can communicate with those nodes in its radio range and thus connect to the network automatically. [9]
- MANET pretense a number of challenges to security solutions due to their diverse resources, severe resource constraints, unclear line of defense, shared wireless medium, dynamic network topology and wireless shared medium. [9]
- The challenges are to find services dynamically for wireless devices, to enable service discovery in a huge MANET. [9]

1.5 Problem Identification

In the previous work [10], we have proposed a swarm intelligence based service discovery mechanism. In this mechanism routing is done by complex interaction of forward and backward network exploration agents (ants).The backward ants uses the useful information gathered by forward ants on their way from source to destination. This raw information is utilized by the backward ants as trip times and further used for updating the routing table of the nodes. The probability is added to nodes in order to find next hop to the destination. The data packets for the next hop are selected with the highest probability. Node routing updates are not performed by forward ants. However, the method fails to address the failures of nodes along the routing path. If any service provider node or intermediate node tends to fail, all the associated service requests cannot be served.

Yet, the service discovery mechanism in MANET endures more security attacks while discovering services. Further, mobility of nodes put forward more issues while considering security in service discovery. Thus, to provide an ideal solution, we propose a Trust Based Security Mechanism for Service Discovery in MANET.

2. RELATED WORK

Jiang Zhong et al. [11] have proposed a cross layer based service discovery protocol known as Cross-layer AODV (CAODV). Their proposed technique can effectively lessen the communication cost. In the same way, they have integrated

CAODV with security certification defined as SCAODV protocol. Their SCAODV efficiently prevent the redundancy of network traffic incurred by the service broadcast processing of service discovery protocol. Thus, their method offers load balancing and on the other hand, their mutual authentication mechanism endows security in the dynamic environment.

Roshni Neogy et al. [12] have presented a novel service discovery protocol. Their protocol has utilized Mobile Agent based System (MAS). These mobile agents choose their route dynamically and exchange service information with the nodes in order to speed up the process. MAS include a set of various groups of agents. Every group is maintained by a unique node termed as owner. The agent collects information about different service providers (SP) and nodes and then disseminates theses informations to the nodes they visit. Further, the nodes share their knowledge with the agents thus enabling them (agents) to predict about unknown service providers without visiting them. Thus, their algorithm is modelled to provide high reliability without regard of network dynamicity.

A lightweight, privacy preserving and secure service discovery protocol is proposed in [13] for ubiquitous computing environment. Their protocol differentiates the service group into two as public service and private service to offer privacy to the users. Further, they have presented mutual authentication and entity anonymity scheme that guarantees non-linkability, security margin, accountability and differentiated access control. The authors have designed their protocol for offering security services in middleware. However, this model can also be used for constructing a security framework adapting its security service to end users' circumstances while conserving a certain security level.

Haitham Elwahsh et al. [14] have proposed a service discovery protocol with security features called as Secure Pervasive Discovery Protocol (SPDP). Their proposed protocol is fully distributed, where services are provided by devices and it can be discovered by others without the need of a central server. It is based on One Way hash Chains, as well as protection of confidential information, secure communications, or access control and compared this with Pervasive Discovery Protocol PDP.

Seyed Amin Hosseini Seno et al. [15] have proposed a Secure Hierarchical Service Discovery and Advertisement Protocol, described as SHSDAP. It is proposed for Cluster Based Mobile Ad hoc Network. This protocol can be applied to routing layer protocol in order to lessen overheads. Further, they have used the distributed directory strategy for service information accumulation and discrimination. In their technique, Cluster Heads (CH) are defined as Certificate Authority (CA). Every time a node tries to join a cluster and starts to negotiate with the CH, it registers itself in the CH as a member. There is an expiration time declaration for every registration record, which is renewed with a single Hello Message (HM). The expiration time out means that the member has left and the record should be removed. When a node changes its status to a cluster head, it sends a message to all the other cluster heads in order to register itself with them.

Sheikh I. Ahamed and Moushumi Sharmin [16] have introduced a trust-based secure Service discovery model, TSSD (trust-based secure service discovery). Their model is modelled for pervasive environments. Thus, the computation and communication are accomplished by nodes themselves deprived of centralized controller. Their model is hybrid and so it permits both secure and non-secure discovery of services. This service discovery mechanism allows sharing of devices considering mutual trust among them. Their model also copes with communication and service sharing security issues.

3. PROPOSED SOLUTION

3.1 Overview

In this research work, we propose a trust based security mechanism for service discovery in MANET. The proposed mechanism estimates confidence/trust value for every node considering its interaction and behavior in the network. Based on security requirements, services are allocated into three ranges of protection level. Services that lie between 0-4 range does not require any secure communication, range 5-7 necessitates moderate secure communication. Finally, range 8 and greater services are highly sensitive services and they are in need of stringent security. For every range of protection level, nodes with particular confidence value are assigned. The confidence value is updated periodically to offer efficient trust model. Further, a technique to establish a secure communication channel is proposed. This technique makes use of offline authority to distribute nodes with secure keys. Thus, the mechanism offers trust based security to service discovery in MANET and guarantees both reliability and security at hand.

3.2 Service Based Trust Model (SBTM)

The trust model is collaborated with Service Discovery Component (SDC) of our first paper [10] to facilitate security in the network. The service based trust model computes the trust value for every node in the network considering their behavior on the service provider or service requester. The SBTM defines two sorts of confidence values (CV) namely common confidence value (CCV) and service specific confidence value (SCV). Here the CV refers to trust level that a node has on other node. CCV is employed in cases such as a node does not have any prior relationship with particular node.

Confidence value (CV) takes three levels as 0.0, 0.5 and 1.0. Here, 0.0 represents lowest confidence level, 0.5 is the average or common confidence level and 0.1 symbolizes the complete and highest confidence level. Fig-1 represents the confidence levels.

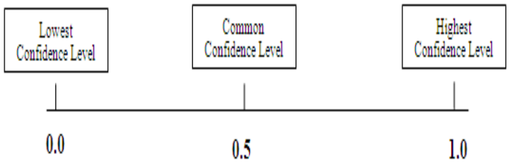

Figure-1 Levels of confidence

Initially, for every service, each new node is allocated with the CV of 0.5 as there is no more information is available to decide its confidence level. $CV(X,Y,1.0)$ is the function that represents the node X has complete trust on node Y for all services and $CV(X_S,Y,S_x)$ describes the confidence value from node X to Y for a specific service **S.** (i.e) The service S is owned by node X, which is represented as OW(S,X) and CV is depends on the confidence level of S_x such as ($0.0 \geq S_x \leq 1.0$). Every node has the privilege to have trust or distrust on their neighboring nodes.

The confidence level (CV) among nodes relies on the following three properties

(i) Reflexive:

Every node has full confidence on itself. This property can be described as,

$$\forall X CV(X,X,1) \quad (1)$$

(ii) Mutual Trust

If a user has more services such as S_1, $S_{2,}S_{3\ldots}$ S_n, then we can assume that the entire services have complete confidence on each other. This is given as,

$$\forall S_1,S_2(OW(S_1,N_i)\wedge OW(S_2,N_i))\Rightarrow CV(S_1,S_2,1) \quad (2)$$

(iii) Partially Transitive:

Suppose node X trusts node Y and in the same manner node Y trusts node Z, then node X also trusts node Z. However, the confidence level (CV) between node X and Z may vary. This property is depicted as,

$$CV(X,Y,1)\wedge CV(Y,Z,1)\Rightarrow CV(X,Z,S_x) \quad (3)$$

$$CV(X,Y,S_x)\wedge CV(Y,Z,S_y)\Rightarrow CV(X,Z,S_z) \quad (4)$$

$$S_z = \vartheta(S_x,S_y) \quad (5)$$

$$0.0 \leftarrow S_x,S_y,S_z \leftarrow 1.0 \quad (6)$$

Apart from above mentioned three properties, confidence value on nodes are service dependent and context awareness.

Typically, all services in the network do not require the same level of protection or security. Security level of each service depends on its application requirement. For instance, some services can be used in military filed that have need of high level of security and commercial services may not prerequisite stringent security level. By exploiting this information, our SBTM assigns various security levels to different services based on their application necessity. The level of security is keep tracked in SerVTable, which has the information about the services as specified in [10].

In this scheme, we use the term protection level to refer security level of services. The scheme describes three protection ranges. First, 0-4 range, services that lies within this range does not necessitate any security or secure communication with service requester. Therefore, these services can be shared with any number of nodes and also with node that have less CV. Secondly, the range that has protection level 5-7. In this range the services demand secure communication and the services can be shared with the nodes that have CV value 0.5 and greater. The final range has protection level 8 and greater value. The services included in this range are highly sensitive services. Therefore, these services can be shared only with the nodes that have CV greater than or equal to 0.8. The protection level assigned to the services is liable to change based on user requirement. The summarization of protection ranges is given in table-1.

Table.1
Protection Range Of Services

S.No	Protection Range of Services	Security Requirement	Sharing with Nodes
1.	0 to 4	No secure communication	It can be shared with any nodes
2.	5 to 7	Secure communication	Nodes with CV 0.5 and greater value
3.	≥8	Highly sensitive secure communication	Nodes with CV ≥ 0.8

3.2.1 Confidence Value Computation

When SDC receives the service request from a node, it exploits the information from SerVTable and Server table. It looks in SerVTable to know whether the node has any specific confidence value for that particular service. If not the SDC computes the common confidence value (CCV) as,

$$CV(SP,X)=\left(\sum_{i=1}^{n} P_i * CV(SP_i,X,a)\right) / \sum_{i=1}^{n} P_i \qquad (7)$$

In the above equation, SP denotes the service provider, $CV(SP,X)$ symbolizes the CCV value of node X corresponding to the service provider SP_i. P_i is the protection level of node i and $CV(SP_i,X,a)$ is the confidence value of node X for the specific service. The value n denotes the total number of services that joins service provider and node X.

Equation (7) is used to calculate the CV value for nodes that already have communication with neighboring nodes. In order to estimate the CV for any new node SDC makes use of equation as follows,

$$CV(SP,New-N)=\left(\sum_{i=1}^{n} CV(SP_i,i)\times CV(i,New-N)\right)/n \qquad (8)$$

Here, *New-N* is the new device that requests service and $CV(i,New-N)$ is the confidence value of node i intended for node *New-N*. While estimating confidence value for new nodes, the SDC receives recommendations from other nodes and service providers. Based on the feed it has received the CV is assigned. On failing to get feedbacks from nodes, the SDC sets the CV as 0.5, which is the common or average confidence value (CCV). This value is selected carefully so that the new node cannot access highly sensitive services and it can obtain services that do not require secure communication. Further, the CV value is dynamically changed according to the behavior of nodes associated with their neighbors in the network.

The confidence value (CV) of node on another node is updated by considering three states as profit, unbiased and loss. Among these three states, profit refers to the increase in the CV value, unbiased means no changes in CV and loss denotes the decrease in CV value. To accomplish and evaluate these three states, SDC defines the common service time (CST), which is the sum of service request time and service offered time. In addition to this, SDC monitors the time when a node transmits a service request, service offered time and the total time needed to complete the service request. This combined value is compared against CST. This value has a main impact on updating CV of a node. The CV of node Z is updated as,

$$CV(SP, node\ Z) = CV(SP, node\ Z) + \eta_i \qquad (9)$$

Where,

$$\eta_i=(\delta_a-\delta_r)/\delta_a \qquad (10)$$

Thus,

$$CV=\frac{\sum_{i=1}^{n}\eta_i * PL_i}{n}\pm J \qquad (11)$$

Here, the modification value of service i is denoted as η_i, δ_r is the necessary time for a successful completion of a service request, δ_a symbolizes the common service time and J is the arbitrary behavioral variable. This variable reveals the behavior of a node like transmitting as much of service requests in a minimum amount of time and forwarding requests to the SDC many times even after the rejection of the particular service request. The value of J can be obtained as,

$$J=(N\_A/(N\_R+N\_E))-(N\_S/N\_R) \qquad (12)$$

Where, N_A, N_R, N_E and N_S represent number accepted service requests, total number of service requests, number of rejected service requests and number of same service requests respectively.

3.2.2 Trust Based Service Assignment Algorithm

The services are discovered by nodes using Swarm Intelligence Based Service Discovery Architecture (SISDA) of [10]. While receiving the service request, the SDC checks the CV and protection level of service that the node requested. When the protection level is lesser than 5 and CV of a node is greater than 0.2 then the corresponding service is granted to node. In cases such as, if the protection level of a service lies between 5 to 7 then the CV of a node is verified. Based on CV value, the decision of permitting or prohibiting the service is taken. When protection level is greater than 7, the similar mechanism as of protection level 5-7 is followed. For the services that have protection level lesser than 5, CV value is not considered, since it does not require secure communication. For every service request, the secure communication channel is established between the service provider and corresponding node. The secure communication channel exchanges a pair of keys between them, which is discussed in section (3.3)

The algorithm for trust based service assignment scheme is given below.

Algorithm-1

Trust Based Service assignment

```
1. Let $CV_i$ be the confidence value of node i
2. Assume that the information about the services is saved in a table termed as SerVTable
3. Let $PL_i$ be the protection level of service $S_i$
4. Service request of node i arrives to SDC
5. SDC checks $PL_i$ and $CV_i$ in SerVTable
// Case-1
        6. If ($PL_i < 5$ && $CV_i > 0.2$ ) then
                6.1 $S_i$ is granted to node i
        7. Else
                7.1 $S_i$ is prohibited to node i
// Case-2

        8. If ($PL_i$ is between 5-7) then
                8.1 SDC estimates $CV_i$ of node i
        9. If ($CV_i \geq 0.5$) then
                9.1 $S_i$ is granted to node i
        10. Else
                10.1 $S_i$ is prohibited to node i
// Case-3

        11. If ($PL_i > 7$) then
                11.1 SDC calculates $CV_i$ of node i
        12. If ($CV_i \geq 0.8$) then
                12.1 Feedback from node i is obtained
                12.2 Based on positive feedback $S_i$ is granted to node i
        13. Else
                13.1 $S_i$ is prohibited to node i
        14. End if
```

3.3 Secure Channel Establishment

Assume an Offline Authority (OA) in the network to distribute nodes with secure keys and to create secure channel among them. In this technique a pair wise key is generated based on RSA algorithm. To accomplish secure communication channel between nodes, the OA certificate along with session keys are used. The distribution of certificates to nodes in the network is illustrated in Fig-2. We assume that before nodes are deployed in the network, every node is assigned with the certificate and secure keys. The OA certificate includes information as per x.509 protocol and it also contains public key information. The OA certificate is encrypted using the private key of offline authority.

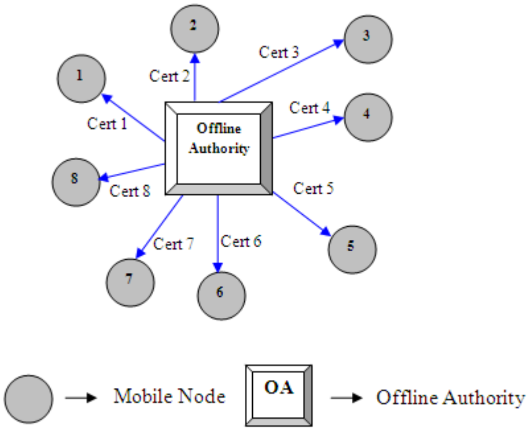

Figure-2 OA distributes certificate to nodes

Consider node X as a mobile node in the network, then OA distributes certificate to node X as follows,

$$OA \rightarrow Node\ X\!: \ Pu_X, \Pr_X, K-OA(Cert_X), K-OA \quad (13)$$

By receiving the certificate, the node decrypts it using OA key and retrieves public (Pu_X) and private key (Pr_X) information. These pair wise keys are utilized to create secure communication channel between two nodes.

Every node constructs a node set (NS) using received HELLO messages. The constructed NS is a table that contains upstream and downstream nodes detail. For every node in NS, the node creates session key to perform secure communication. The construction of secure channel between *node X* and *node Y* takes the following steps as follows,

1. To begin with, node X constructs REQ message to node Y. The REQ message is encrypted using private key of node X (Pr_X) and the entire message is protected through the certificate of node X.

$$Node\ X \xrightarrow{REQ} Node\ Y \qquad (14)$$

$$REQ: (Pr_X(REQ)Cert_X)$$

2. While receiving the REQ message, node Y authenticates the certificate of node X and decrypts the REQ message via the public key of node X (Pu_X). And then, it generates the session key between itself and node X and places the information in ACK message. Once the ACK is constructed, it is encrypted through private key of node X and the entire message is protected through the certificate of node Y. Then the ACK packet is forwarded to node X.

$$Node\ X \xleftarrow{ACK} NodeY \qquad (15)$$

$$ACK: (Pu_X(ACK, SeS_{X\text{-}Y}),Cert_Y)$$

3. On receiving ACK, node X authenticates the packets and decrypts it using its private key and retrieves the session key ($SeS_{X\text{-}Y}$).

Thus, the generated session key is used between node x and node Y for data transmission, which creates the secure communication channel. The pair wise keys (private and public keys) are updated periodically to prevent hacking of keys and nodes. This is achieved through maintaining timer for a key pair. Once the timer gets expired, the newly generated keys are transmitted by encrypting it with the old public key of the corresponding node.

4. SIMULATION RESULTS

4.1. Simulation Parameters

We evaluate our Trust Based Security Mechanism for Service Discovery (TBSMSD) through NS-2 [17]. We use a bounded region of 1000 x 1000 sqm, in which we place nodes using a uniform distribution. The number of nodes is 40. We assign the power levels of the nodes such that the transmissions range as 250 meters. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The simulated traffic is Constant Bit Rate (CBR).

The following table summarizes the simulation parameters used.

Table 2
Simulation Parameters

No. of Nodes	40
Area Size	1000 X 1000sqm
Mac	802.11
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512.
Transmission Range	250m
Rate	100Kb.
Attackers	2,3,4,5 and 6

4.2. Performance Metrics

We compare the performance of our proposed TBSMSD approach with SISDA [10] technique. We evaluate mainly the performance according to the following metrics:

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Throughput: It is the average number of packets received per receiver

Drop: It is the total number of packets dropped during the data transmission process.

The simulation results are presented in the next section.

4.3. Results & Analysis

In our experiment we measure the above metrics by varying the number of attackers as 2,3,4,5 and 6.

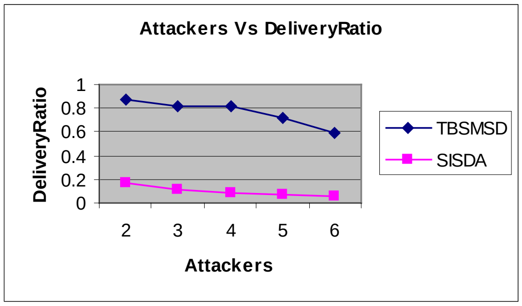

Fig. 3.Attackers Vs Delivery Ratio

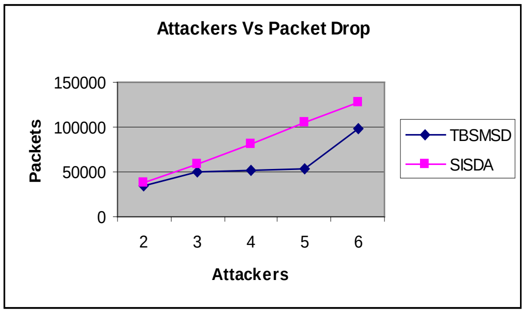

Fig .4.Attackers Vs Drop

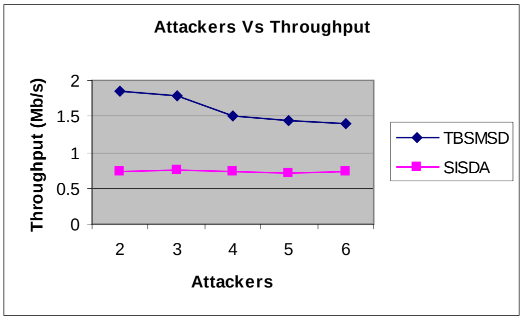

Fig .5. Attackers Vs Throughput

When the number of attackers is increased, the packet drop will be increased leading to degrade of throughput and delivery ratio.

Fig 4 shows the packet drop occurred for both the schemes. We can see that the packet drop of TBSMSD is less than the existing SISDA method, since it detects and eliminates the attackers.

Fig 3 and 5 show the packet delivery ratio and throughput of both the schemes, respectively, when the attackers are increased. We can see that the throughput and delivery ratio of TBSMSD is higher than the existing SISDA technique.

5. CONCLUSION

In this research work, we have proposed a trust based security mechanism for service discovery in MANET. The mechanism computes confidence/trust value for each node considering its interaction and behavior in the network. And also the trust model designates different protection level for services. Based on security requirements, services are allocated into three ranges of protection level. Services that lie between 0-4 does not require any secure communication, range 5-7 necessitates moderate secure communication. Finally, range 8 and greater services are highly sensitive services and they are in need of stringent security. Considering protection level of the services secure communication is offered. Further, the secure communication channel is established among nodes by sharing secret keys. By simulation results, it has been shown that the proposed mechanism provide better security against attacks with reduced packet drops.

REFERENCES

[1] Moussa Ayyash, Donald Ucci and Khaled Alzoubi, “A Proactively Maintained Quality of Service Infrastructure for Wireless Mobile Ad Hoc Networks”, *International Journal of Communication Networks and Information Security (IJCNIS) Vol. 2, No. 2, August 2010*

[2] Lovdeep Grover, Lal Pratap Verma, and Aniket Mathuria, “Comparison between SAR and NSAR in MANETs”, *International Journal of Data & Network Security, Volume 1 No.1, August , 2012*

[3] Mamoun Hussein Mamoun, “A New Reliable Routing Algorithm for MANET”, *International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 3, June 2011*

[4] Zhenguo Gao, Ling Wang, Mei Yang and Xiaozong Yang, “CNPGSDP: An efficient group-based service discovery protocol for MANETs”, *Elsevier, Computer Networks, pp- 3165–3182, 2006*

[5] Yuan Yuan and Ashok Agrawala, “A Secure Service Discovery Protocol for MANET”, *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, (PIMRC), Vol.1, pp- 502- 506, 2003.*

[6] Christopher N. Ververidis and George C. Polyzos, “Service Discovery for Mobile Ad Hoc Networks: A Survey Of Issues And Techniques”, *IEEE Communications Surveys, 3rd Quarter 2008,*

[7] Noor Mohd and Quamar Danish, “A Proposed Model for Service Discovery with Security in Wireless Adhoc Network”, *International Journal of Scientific and Engineering Research, IJSER Volume 3, Issue 8, August 2012*

[8] Adnan Noor Mian, Roberto Baldoni, and Roberto Beraldi, “A Survey of Service Discovery Protocols in Multihop Mobile Ad Hoc Networks”, *IEEE Pervasive Computing, 2009*

[9] Rutvij Jhaveri, Kruti Dangarwala and Neha Bhanot, “Security and Service Discovery Issues in Mobile Ad-hoc Networks”, *International Journal of Networking, Volume 1, Issue 1, pp- 01-03, 2011*

[10] S. Pariselvam and R. M. S Parvathi, "Swarm Intelligence Based Service Discovery Architecture for Mobile Ad Hoc Networks" *European Journal of Scientific Research, Vol-74, No-2, pp-205-216, 2012*

[11] Jiang Zhong, Shenghua Geng, Luosheng Weng, and Xue Li, "A Cross-layers Service Discovery Protocol for MANET", *Journal of Computational Information Systems, pp-5085–5092, 2012*

[12] Roshni Neogy, Chandreyee Chowdhury, and Sarmistha Neogy, "A Reliable Service Discovery protocol using Mobile Agents in MANET", *IEEE Reliability and Maintainability Symposium (RAMS), pp-1-7, 2012*

[13] Jangseong Kim and Kwangjo Kim, "A Lightweight, Privacy Preserving and Secure

Service Discovery Protocol in Ubiquitous Computing Environment", *WISA 2008*

[14] Haitham Elwahsh, Mohamed Hashem, and Mohamed Amin, "Secure Service Discovery Protocol for AdHoc Networks Using Hash Function", *International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.4, July 2012*

[15] Seyed Amin Hosseini Seno, Rahmat Budiarto and Tat-Chee Wan, "SHSDAP: Secure Hierarchical Service Discovery and Advertisement Protocol in Cluster Based Mobile Ad hoc Network", *World Applied Sciences Journal, pp- 115-128, 2009*

[16] Sheikh I. Ahamed, and Moushumi Sharmin, "A trust-based secure service discovery (TSSD) model for pervasive computing", *Elsevier, Computer Communications, pp-4281–4293, 2008* .

[17] Network Simulator: http:///www.isi.edu/nsnam/ns