World Applied Sciences Journal 7 (Special Issue of Computer & IT): 115-128, 2009
ISSN 1818.4952

SHSDAP: Secure Hierarchical Service Discovery and Advertisement Protocol in Cluster Based Mobile Ad hoc Network

Seyed Amin Hosseini Seno, Rahmat Budiarto and Tat-Chee Wan

School of Computer Sciences,
Universiti Sains Malaysia, 11800 Penang, Malaysia

Abstract: Mobile Ad hoc Networks (MANETs) have many potential applications in various fields such as military services, collaborative and distributed computing, emergency operations, wireless sensor networks and hybrid wireless networks. Dynamic Service Discovery and Advertisement (SDA) have also brought significant issues to the networking technologies. Since most protocols in mobile ad-hoc network do not have built-in security and all mobile devices communicate with each other through a wireless link without any intermediate infrastructure, security issues must be addressed. Accordingly, all devices should be able to advertise their own services and discover their required services dynamically and safely. Obviously, achieving security goals such as entity authentication, data confidentiality, data integrity, non-repudiation are critical because of the many opportunities for misuse. A Cluster-Based Distributed Certificate Authority (CB-DCA) which is a fully distributed certificate authority protocol is proposed to support the proposed Secure Hierarchical Service Discovery and Advertisement Protocol (SHSDAP). Compared to the APBC and EZRP protocols, it is obvious that SA & SD overhead, routing overhead and energy consumption are significantly lower than for other protocols. Furthermore, in all cases, the SD hit ratio of our proposed protocol is higher than 86%. SHSDAP is secure against attacks and forged identities.

Key words: Service discovery and advertisement . CBRP . MANET . Security . DCA

INTRODUCTION

The number of Mobile Ad-hoc NETwork (MANET's) applications are steadily increasing as mobile devices used as MANET nodes become more feasible. MANET is considered a significant part of 4G wireless technologies [1]. Therefore, using mobile ad-hoc networks, particularly during emergency situations, is becoming a priority. The main focus of this paper is on Service Discovery and Advertisement (SDA) issues with emphasis on Security.

SDA is becoming more and more important in network applications, especially in MANETs. In fact, such considerations are major prerequisites for assuring the efficiency and usability of MANETs [2]. There are many serious challenges to the introduction and implementation of SDA protocols for MANETs, such as limited bandwidth, dynamic topologies, variation in network size, limited physical resources and serious security threats [3].

The issue of security and prevention of misuse and fraud in network applications has always been a major concern. Achieving the security goals for MANETs especially in the case of SDA is a necessity and a high priority.

The limited power supply of mobile nodes is one of the key issues. Thus, any modification such as security enhancement should be carried out cautiously to minimize energy consumption. The energy consumption can be minimized by keeping the number of transmissions low, as used as decreasing CPU and memory usage.

To solve the aforementioned challenges, this paper proposes a Secure Hierarchical Service Discovery and Advertisement Protocol (SHSDAP) based on CBRP and Cluster Based Distributed Certificate Authority (CB-DCA). These protocols are applied to the routing layer protocols to reduce overheads. We use the distributed directory strategy for service information accumulation and discrimination.

To reduce communication overhead and implement Hierarchical SD (HSD) and Hierarchical SA (HSA) we divide the nodes into clusters based on routing layer information. Thus, the protocol minimizes the flooding traffic efficiently during route discovery and speeds up the process as well. The Cluster Based Routing Protocol (CBRP) is a robust and scalable routing for MANETs and is superior to existing methods [4-6]. For example, the overhead of CBRP is less than AODV (a standard routing protocol for MANET) while its

Corresponding Author: Dr. Seyed Amin Hosseini Seno, School of Computer Sciences,
Universiti Sains Malaysia, 11800 Penang, Malaysia

throughput is more than AODV [7]. SHSDAP is based on CBRP and Cluster Heads (CH) are defined as Certificate Authority (CA). Each 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.

Secure Service Advertisement (SSA), Secure Service Discovery (SSD) and the Secure Use of Service (SUS) protocols are built in the CBRP routing protocol to enforce security policies for the MANET.

The organization of this paper is as follows: Section 2: reviews briefly SD in general and SSD in particular. Section 3: presents the statement of our proposal which is offered in three following sub categories: SSA, SSD and the SUS. Section 4: Presents the simulation experiments we carried out and discusses the performances. Section 5: includes the conclusion and future work.

RELATED WORK

SD is not a new issue in networks and many research studies have been conducted in this area. SD protocols can be divided into three main categories. (i) SD support layer based on application or network layer protocols. Konark [8-10], GSD [9, 11] and SANDMAN [12] are examples of application layer SD protocol. SD based on AODV [13], ODMRP [14-16], EZRP [17], DSDP [16] and LSDP [18] are examples of routing layer SD protocols. (ii) SD based on Service directory strategy, containing directory-less, central directory and distributed directory protocols. This category includes UPnP [8, 19], PDP [20], DEAPspace [21], JINI [22], SLP [23], Sailhan [24]. (iii) SD based on Multicast DNS. ANS [25] exemplifies this category.

Some of the above protocols are not suitable for direct use in MANETS, since some protocols like JINI and SLP employ a node as a permanent directory server which contradicts MANET requirements. Some other protocols, such as DSDP which do not use a central directory, normally have high energy consumption and security concerns are not addressed for these protocols.

The basic security goals of SSD in MANETS are entity authentication, data confidentiality, data integrity, non-repudiation and freshness during the communication among servers, agents and clients. These basic security goals can be carried out by applying standard cryptographic techniques [26] using session, public and private keys for encryption and certificate mechanisms for SA and SD in a hierarchical network.

The following is a review of several protocols:

Yuan Yuan Arbaugh *et al*. [27] proposed a Dynamic Service Discovery Protocol (DSDP) which is a routing layer protocol. In this proposal SD is based on a pull model which uses hash functions and message authentication codes (HMAC).

Todd D. Hodes *et al*. [28] proposed a Service Discovery Service (SDS) which is an application layer protocol. It has five main components: SDS servers, services, clients, capability management and certificate authority. The SDS encrypts all information which is exchanged between system components and uses cryptographic methods to provide strong authentication. To reduce overhead of decryption, symmetric-key cryptography is used.

Feng Zhu *et al*. [29] introduced a proxy based approach to establish a secure and trusted relationship between communication parties.

Almen´arez *et al*. [30] proposed a Secure Pervasive Discovery Protocol (SPDP) which is a distributed protocol. SPDP provides security based on existing protocols and an anarchy trust model using Public Keys Infrastructure (PKI). In this protocol every node has some memory to contain a list of trusted nodes and a list of services belonging to trusted nodes.

Scholten *et al*. [31] introduced a SSD protocol for home networks which uses a secret session key protocol for the authentication and integrity proof of transferred messages.

Renwei Ge *et al*. [32] introduced "Secure Indirect-Address Service Discovery in MANET". In their paper, a framework was defined to apply the Chord protocol into SD in MANET and secure it against Byzantine attack. Message authentication was secured in three stages: Secured RREQ message, Secured RREP message and Secured Multiple-Destination-RREQ (MD-RREQ) message. The destination can verify the received MD-RREQ by using the source's public key.

The Splendor protocol [33] focused on security and position awareness. The main components of Splendor protocol are client, mobile service, directory, proxy and third-party server. In this protocol mobile services authenticate with proxies and ask proxies to handle registration, authentication, authorization and key management for them.

As mentioned in previous sections, there are few secure SDs in dynamic networks. In this type of network, secure SD is a challenging issue. Some of the above protocols such as [27, 30] try to have a secure SD but the security is problematic. Since there are no certificates and certificate authorities. Some other

protocols such as [28, 29, 33] use a central server as a certificate authority which is a challenging issue for MANETs, causing more messaging overhead in the network and consumes more energy as a result. Although some protocols such as [27, 32] were designed for layer two protocols, thus minimizing overheads, they do not introduce a comprehensive security architecture due to a lack of suitable key signature management in the network.

There are several papers on distributed certificate authorities such as: Zhou *et al*. [34] which proposed a multiple-key cryptography-based Distributed Certificate Authority (DCA) scheme (MC-DCA), based on threshold cryptography to solve the problem of Sybil attacks in DCA.

These protocols add high messaging overheads to the network. To reduce message overheads in the network, we propose SHSDAP based on CBRP. Obviously, in a dynamic network, cluster-based networking protocols have minimum message communication overhead compared to other types of protocols. Thus, by employing a cluster based network topology and designing a light weight security architecture with suitable distributed certificate authorities the proposal causes only a minimal increase in overhead to the network.

The protocol was compared with EZRP and APBC for SD and security issues respectively. Both of them are structurally similar to our work. A review of CBRP, EZRP and APBC is presented in the following sections.

Cluster based routing protocol: Each protocol has its benefits and drawbacks and cannot be claimed to be absolutely better than the other. A. Boukerche in [35] has done a performance comparison between CBRP, AODV and DSR by simulating these protocols in NS-2. This comparison has been done through various sources and mobility based on three performance metrics: throughput, overhead and delay. The number of node population is 50. The traffic and mobility is the same as C.E. Perkins *et al*. in [36] which is a common test scenario. Traffic source is CBR and the maximum speed is 20 m/sec. The result of this study shows that throughput of CBRP is higher than AODV. Although HM overhead in CBRP is considerable, A. Boukerche's study shows that overhead of CBRP is less than AODV. N. Moghim *et al*. in [7, 35] have proved these issues. What is notable is the AODV nodes that help in sending and receiving data and control pack*et al*so uses HM. It should be motioned that AODV exhibits a very short end-to-end delay.

Based on the above characteristics and studies being done by [4-6], the CBRP as a routing protocol designed for medium to large MANETS is a robust/scalable routing protocol.

Zone Routing Protocol (ZRP): Zone Routing Protocol (ZRP) is a hybrid routing protocol designed for mobile ad hoc networks. The protocol divides the ad hoc network nodes into a number of overlapping zones. It is either a proactive or a reactive protocol. It has some sub protocols doing certain functions as follows: (i) Intra zone Routing Protocol (IARP); (ii) Inter zone Routing Protocol (IERP); (iii) Neighbor Discovery Protocol (NDP); and (iv) Broadcast Resolution Protocol (BRP) [17, 37, 38]. EZRP or Extended ZRP adds support for service discovery and advertisement.

Authentication Protocol Based on CBRP (APBC): Lee *et al*. [39] have proposed APBC. The authors composed Cluster Based Routing Protocol (CBRP) by the use of multi-layer. To elect Cluster Head (CH) in APBC the least cluster change (LCC) algorithm is employed [40]. In this protocol a Master Cluster Head (MCH) is defined as a CA which manages all the others. This is because each communication needs to get a certificate from the MCH.

PROPOSED SHSDAP

Although public key method is more suitable to secure information, it has some limitations. An example is that users must trust a given certificate authority. Of course, this requirement is present even for real world environments such the banking system.

In this paper, we propose a new distributed certificate authority mechanism called Cluster-Based Distributed Certificate Authority (CB-DCA) and a secure cluster based hierarchical service discovery and advertisement based on CB-DCA. In addition, SSD is based on a public key system mechanism.

A distributed certificate authority mechanism for SHSDAP: As has been stated in previous sections, one of the important issues to sustain security in general and SSD in particular, is the use of Certificate Authority (CA). Employing CA in ad-hoc networks is not only a very difficult undertaking but also adds more messages overhead to the network. In our proposal, we try to avoid such overheads and create an effective CA. One of the requirements in this framework is to define an Offline Office (OO) near our network. It is an efficient aspect of energy consumption and process speed. In other words, we tried to move some functions from ad hoc network nodes to this center. Figure 1 shows that every node which is supposed to be a member of an ad hoc network should get an offline certificate and keys from the Offline Office installed before joining the ad hoc network. The OO assigns the certificate and keys to the nodes via physical media such as pen drives (in offline mode). A malicious node lacking a

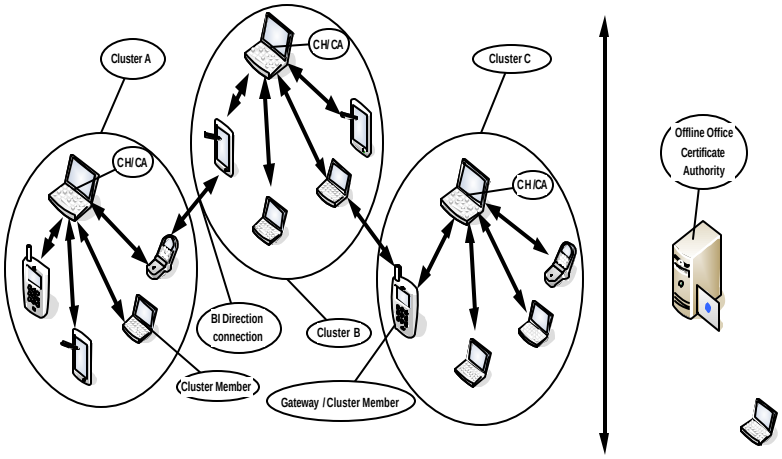


Fig. 1: Sample of secure ad hoc network

Table 1: Notations used in SHSDAP protocol

Notation	Description
OO	Security office identity
CHx	Cluster Head identity x
CH	Local Cluster Head
CM	Cluster Member
MNU	Undecided mobile node identity
ACK	Acknowledge
Req	Request
MNx	Mobile Node X
K-x	Private key of X
K+x	Public key of X
K-(…)	Message encrypted using private key
Certx	Certificate of X
MNMx	Member mobile node identity
SKx-y	Session key between x and y
SKx-y(…)	Message encrypted using session key
A→B: C, D, …	Node A transmits the C, D, … to Node B

certificate from the security office cannot connect to the network even if it is inside the coverage of network nodes. The tasks of OO center are:

- Full security checking to the nodes before connecting to the network.
- Creating a pair key (private and public) based on RSA algorithm.
- Creating a certificate for the nodes based on x.509 protocol which contains version, serial number, validity period, issuer name, signature algorithm identifier, subject name and subject public key information.
- Encrypting the certificate with its private key and passing it to the nodes.
- Passing the keys and certificate to the nodes (Table 1 for notations):

OO→MNU: K+MNU, K-MNU, K-OO (CertMNU), K-OO

- Recording the nodes information such as MAC address and public and private key.

Hypotheses

- Each node which wants to be a valid node in a network and wants to have an effective communication, should take an offline certificate along with a pair of keys (public and private keys) from the OO before connecting to the network. The life-time of keys is a working session in a network. OO generates a pair key and encrypts it with the old public key of the node and sends them after life-time of nodes is expired.
- If a node does not take a certificate, based on the proposed scheme, it cannot do anything in the network.
- Only the nodes which have a certificate from the offline office center can become CH node.
- An offline certificate contains information based on x.509 protocol, plus the node's public keys.
- Before passing certificate to the node it should be encrypted with the OO's private key.
- A node can trust the offline office public key and other nodes to have a certificate.
- The Security office has a wireless link for sending the new keys and certificate after they have been expired.

Based on our proposed protocol, the network consists of a set of clusters with dynamical membership, where nodes get certificate and keys use the OO. The nodes which get certificate from OO can become CHs (having certificate condition is added to the elect CH rules in CBRP). Therefore, CH which plays the role of CA is a valid and safe node. The nodes introduce and register themselves to the CHs and become a member node, if no problem 0ccurs. Since all traffic between clusters is transferred via CHs, CH is an appropriate node for processing node certificates. After establishing the certificate and keys by the CHs a secure channel is created with a generated session key for securing communication between two nodes. Consequently, CH acts as a CA in this process without sending or receiving any packets other than normal CBRP control packets (sending data and authority checking are done simultaneously) and also the information is transferred via a secure channel. In fact, our algorithm avoids message overhead that is generated by sending request to a central CA such as for APBC or by using the threshold cryptography mechanism such as MC-DSA. If by any chance, CH is disconnected from network, based on CBRP, a neighboring node having a valid certificate will be elected as the CH, the information of the CH is updated as soon as it receives the first HM. All keys and certificates are valid for a working session. Before certificate expiration, the security office will generate a key pair and a new certificate and then encrypt them with the node's previous public key and sends them to the node via its wireless link.

Secure cluster formation: Based on CBRP, each node has three states: cluster member, CH and cluster undecided. All nodes wake up in the undecided state. Each node has a Neighbor Table which is used for gathering cluster related information [5], including NEIGHBOR_ID, LINK_STATUS and ROLE. To facilitate cluster formation, each node uses the information obtained from the HMs. HM is generated based on the steps as follows: (i) Collect information of node based on CBRP HM structure. This information consists of the Neighbor Table, Adjacency Table [5] and service information, (ii) Encrypt the information with private key and add it to HM, (iii) Add certificate of node to HM and (vi) Broadcast the HM. An undecided node broadcasts the HM periodically based on its timer. When a CH receives a HM from an undecided node, it decrypts the certificate and based the on certificate information, decrypts the other information within the HM and updates its table. If there is no problem with the certificate, it sends out a triggered HM which is encrypted using the node's public key immediately. If an undecided node receives a HM from a CH, it means that there is a bi-directional link in between them. It aborts its timer and sets its own status to become a cluster member and update its neighbor table. If the timer times out, the node re-enters the undecided state; if the node's Neighbor Table contains no bi-directional neighbors otherwise it elects itself as a CH. The other roles are the same as for CBRP. If there were any problem with the certificate, the CH will drop the received HM (see the following steps: "Tables Info" consist of Neighbor Table, Adjacency Table [5] and services information):

MNU→CH: K-MNU(Tables Info), Cert MNU

CH→MNU: K+ MNU(HM), Cert CH

When an invalid (unauthorized) node enters a network, it will not be able to start an effective connection because: (i) it does not have a certificate from the offline office (CA) and (ii) it does not have an offline office public key from the offline office (CA) to decrypt the certificates. Therefore, this protocol not only prevents an unauthorized node to connect to other nodes, but also prevents it from extracting and receiving other nodes' packets because they are encrypted by both offline CA key and the sender's key. During the node life-time, when the timer of HM overflowed or a node is in an undecided status, the node also creates a HM by adding encrypted current tables with node's private key and certificate to it and broadcasts it. In receiving HM by node, if there is any problem with the security in each of check step, packet will be dropped.

In order to create a secure connection between the two nodes in the network, the steps are shown in Fig. 2 that shows inside the cluster connection (local connection) and Fig. 3 that shows a connection between two nodes of different clusters.

To implement a secure Protocol, the following issues would be addressed: SSA, SSD and SUS. These will be discussed in detail in the following sections:

SSA: In order to add SA capability to CBRP, it needs to store the service attributes on the network. To achieve this, a new table called Service Access Table (SAT) is deployed. Accordingly, each node now has a SAT for storing all the available services. For every service, information such as service ID, type of service, owner of service and some attributes are stored in the SAT. SAT updates when a service is added to a machine located within the ad hoc network environment and the owner then based on some criteria decides whether to share the service or not.

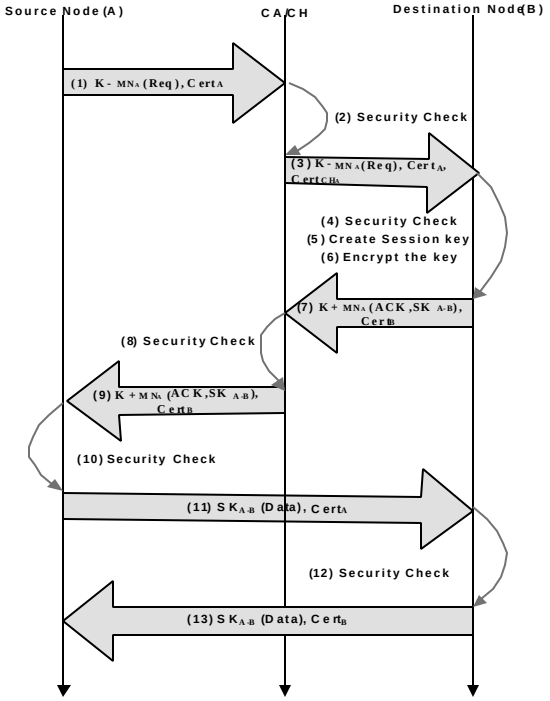


Fig. 2: How to create a secure connection inside the cluster

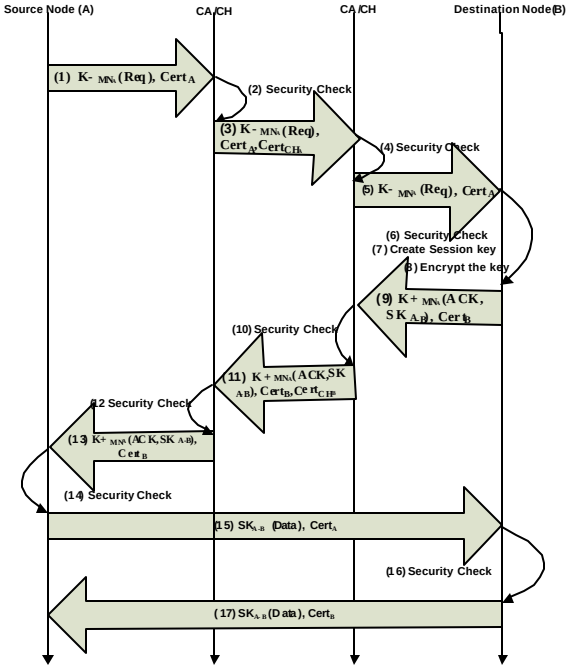
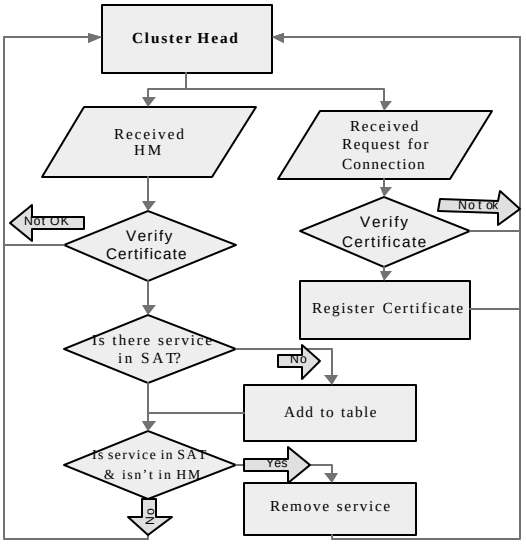


Fig. 3: How to create a secure connection between clusters



HM: Hello Message, SAT: Service Access Table

Fig. 4: Cluster head state transition diagram for SA

As mentioned before, when a node shares a service, it stores the service in its SAT and sends it to CH by creating a packet which contains the SAT called Update packet (UP) with a unicast service if the time spent on previous HM is less than half of the HM period time (MNMx→CH: K+CH(UP), Certx). On the other hand, to enable CBRP to contain SA, a new HM packet has been organized for CBRP. In fact, we use the CBRP HM with some additional fields: number of services and services parameters based on SAT. Every node in CBRP broadcasts a HM periodically (MNMx →Neighbors: K-x(HM), Certx). When the cluster head receives a packet containing one or more services, after checking the security it should update it's SAT without any imposed overhead. In addition to the periodical HM by client, any change made to the SAT or to the client, requires the client to prepare an UP packet containing the changes that is sent to CH. For example, when a service is deleted from SAT in a member node, the SAT of the CH has to be updated. Therefore, an UP is prepared, encrypted with CH public key and sent with its certificate directly to CH after a secure channel is created. The UP contains the status, number of services and services properties based on SAT. To avoid eavesdropping and any other attack, the node does the following steps: (i) it encrypts the packet with the CH public key and (ii) the encrypted packet and its certificate sent to CH as a unicast (MNMx→CH: K+CH(UP), Certx). This is accomplished based on the procedure mentioned in section 3.1.

Upon receiving a HM packet or any other packet containing one or more services from a CH in the network, the process for authentication and updating is done based on a CH transition diagram (Fig. 4).

The cluster head modifies its own Service Table based on the following algorithm:

- It checks whether services in the HM are already in the Services Table or not. If not, it adds some entries for them.
- If there is an existing service in the SAT that is not included in the HM, the service will be deleted from the Services Table in CH.

We propose a trusted service using information encryption mechanism, certification and session key in order to be able to transport service information securely and to avoid overhearing and service forging in the network.

SSD: Our proposal is a secure HSD. It means that, at the first level, service requester or client searches for the required service within its own SAT. If the queried service is shown to be suitable, it is selected and the discovery process is terminated. In this step no security measurement is taken because the requester contains the required service. If a suitable service is not found, the client will prepare a request packet and encrypts it with the CH public key. The request packet and the certificate are sent to CH as a unicast (MNMx→CH: K+CH(Request), Certx). The CH then does the following steps. As CA, CH decrypts certificate with main CA public key and checks the certificate of the requesting node. If the requester has not been registered yet or if the verification of certificate is not acceptable, CA (CH) drops the request and the process for finding a suitable service is terminated and the requester is added to the black list. If there is not any problem with the certificate, CH decrypts the request using its private key. Subsequently, CH searches for the client's required service within its SAT. If CH finds a suitable service, service properties and the certificate are encrypted with public key of service requester and the packet is sent to the requester (CH→MNMx: K+x(service information), Cert CH).

If no local suitable service is located, the request is sent to other cluster heads. When CH sends a request to the adjacent CHs, the cluster head will follow all steps that a node follows. The adjacent CHs will also follow the same steps that were mentioned for the CH above (CHx→CHy: K+CHy(Request), Cert CHx). Another point to be explained here is that in some instances there are more than one suitable service available for one particular request. All these services are found by the neighbor CHs. The CHs then send all the obtained services to the CH to which the requester is a member. Subsequently, the CH chooses the best service based on some parameters (such as speed, length of queue, locality and distance) and sends it to the requester.

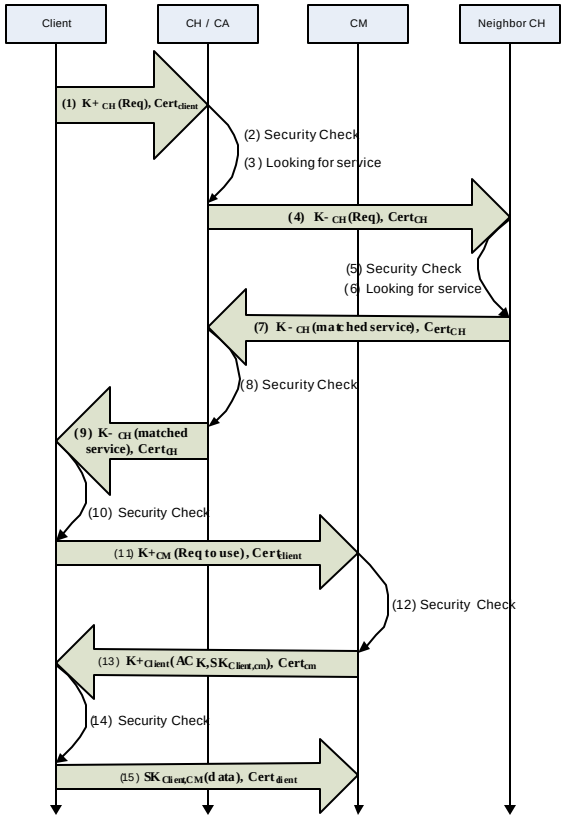


Fig. 5: SD message passing diagram for Non local SD

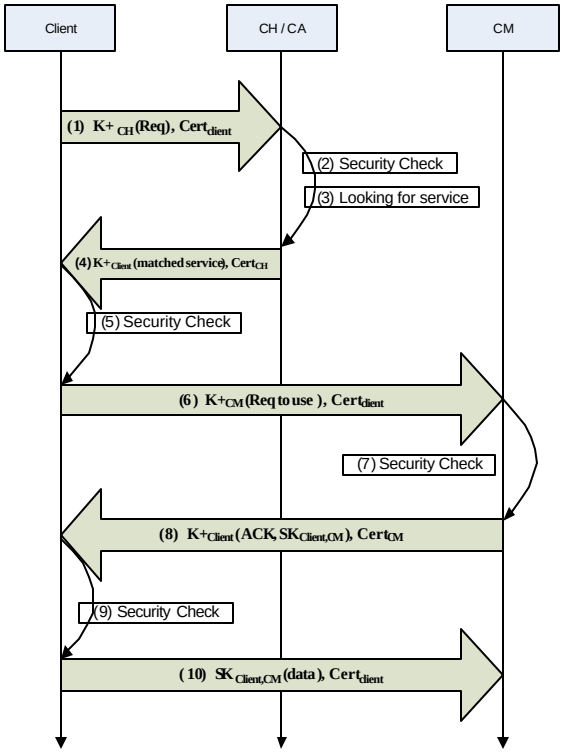


Fig. 6: SD message passing diagram for local SD

Table 2: Simulation setting

Simulation duration	900 sec
Broadcast interval	2 sec
Pause time	2 sec
Maximum speed of the node	10 m/s
Area	Max x = 500 m max y= 500 m
Number of request for service	300
Background traffic	CBR
CBR maxpkts	1100
Max connection	8
Sending rate	0.25
Seed	1.0
Number of nodes	15, 20, 30, 40, 50, 60, 70, 80, 90

SUS: Using a service securely is an important part of our proposal. When a node with new service joins a network and its owner shared the service, in the first step of advertisement, the node sends the service properties to CH. All information transferred between service provider and service requester, based on their public keys, is encrypted and communicated in a secure channel based on a session key (Fig. 5 and 6). We believe that this method is very secure for using data and it is impossible to be attacked. For example, assume we want to send important data to a printer which is in the network. Based on what was mentioned above, print service requester explores the printer properties, then prints requester's encrypted data with a session key (which is sent by service provider) and sends it to printer provider in a secure channel based on a session key. The CH of printer provider authenticates the printer provider and if the certificate is ok, delivers the packet to printer provider. After receiving the packet from printer requester, it decrypts information and if there is not any problem, it sends them to the printer and this scenario will be continued.

The last point of security is that every CH (CA) delivers the packet which comes from a certificated node. In other words, CH/CA checks certificate and other security's parameters for any connection. Our proposal encrypts all data sent between system components. To reduce the overhead of decryption, symmetric-key cryptography is used [41-44].

SIMULATION, EVALUATION, RESULT AND ANALYSIS

Our experiments were conducted in Network Simulator 2 (NS2) [45]. To facilitate the analysis of the results, we assumed that there are 15 services available in the network. The services are first distributed at random among nodes so that each node cannot own more than one service to offer to the other nodes. The scenario files are created by the SetDest tool of the NS2 and the traffic files are created by cbrgen.tcl. The simulation settings and parameters are shown in Table 2. Various existing protocols were evaluated and compared to determine the efficiency of the proposed SHSDAP. CBRP is a cluster based routing protocol without SA & SD or security mechanisms; EZRP is a zone based SD & SA protocol without any security mechanisms; while APBC is a cluster based secure routing protocol. Finally, SHSDAP is a secure cluster based SD & SA protocol.

Since SHSDAP is a cluster based routing protocol that supports SDA in the MANETs, it is necessary to compare it with other protocols that use common techniques when trying to evaluate our protocol. There are a few clusters based routing protocols for MANETs. We found EZRP to be zone based and SD enabled. EZRP is also a zone SD that supports routing. APBC, an authentication protocol that is under the control of CBRP for security and certificate authority, also meets the requirements for our proposal. Consequently, the performance comparison among SHSDAP, EZRP and APBC are presented in this paper.

Performance evaluation: Packet Delivery Ratio is an important parameter for evaluating the function of routing protocol. In the first set of experiments, the Packet Delivery Ratio vs. mobility pause time was evaluated. The Pause time had these values: 2s, 50s, 100s, 150s, 300s, 600s and 900s. We captured the mean of packet delivered in various states vs. pause time in the network. Figure 7 indicates that Packet Delivery Ratio increases with the increase in the pause time.

This demonstrates that in cases of packet delivery ratio and routing control overhead, SHSDAP performs better than EZRP.

SDA side effects comparison: Three performance metrics are evaluated in our experiments. The first performance metric is the total mean of control message overhead in SD mechanism. The control message overhead comprises Hello Messages, Update Messages, Acknowledge messages, etc. This measures the impact of the various algorithms on network resources in terms of the number of packets. The mean of service hit ratio is the second performance metric. Hit ratio is simply the ratio of the total number of successful attempts to the total number of requests. When hit ratio and control message overhead are combined together, it reflects the efficiency of each approach. The third performance metric is the average time delay referring to the time during which a successful request is sent by a client and the corresponding reply is received by the same client.

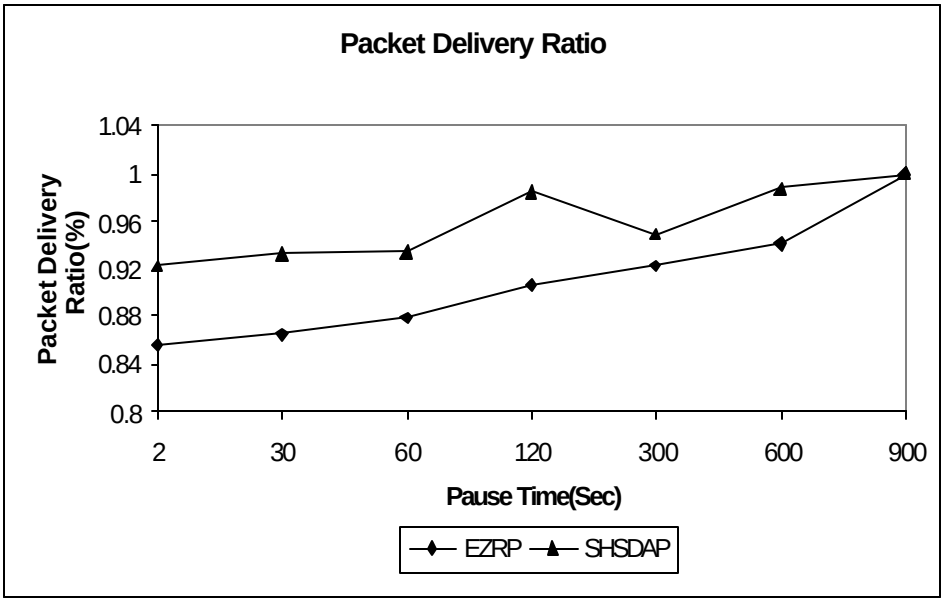


Fig. 7: Packet delivery ratio

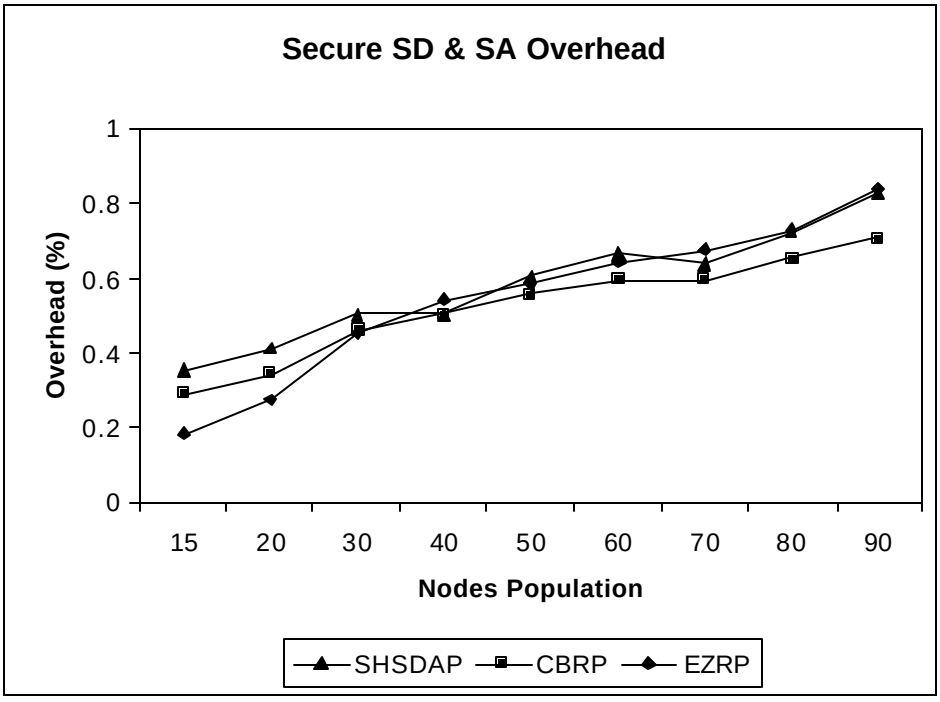


Fig. 8: SSD and SSA overheads

One of the performance metrics is the total mean of overhead of SHSDAP mechanism which measures the load of the algorithms on a network resource in terms of the number of packets. In our experiments, we intended to capture the effect of adding SSA and SSD to the CBRP on controlling message overhead when we increase the number of the nodes. We have separately captured the means of control message overhead for various states in term of the numb er of nodes in the network before adding Secured SA and SSD to the CBRP and after adding SSA and SSD to the CBRP. Figure 8 shows the overheads versus number of nodes for Secured SD.

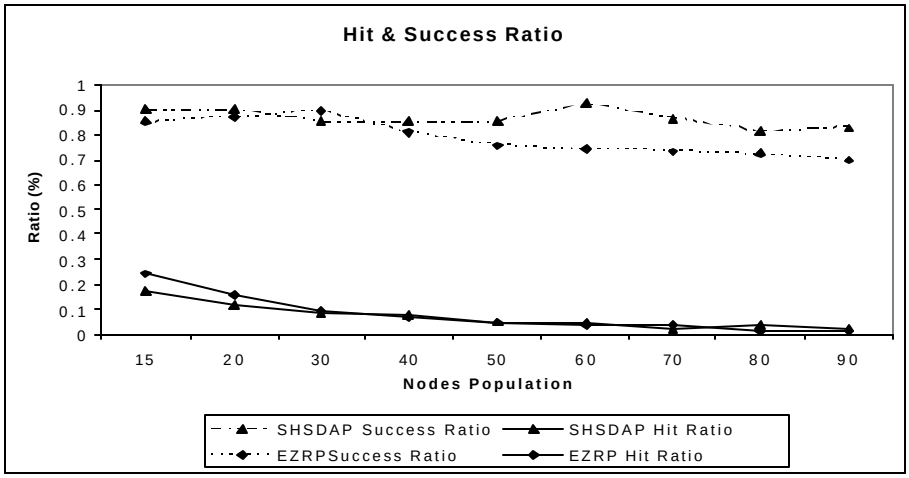


Fig. 9: Service hit and success ratio

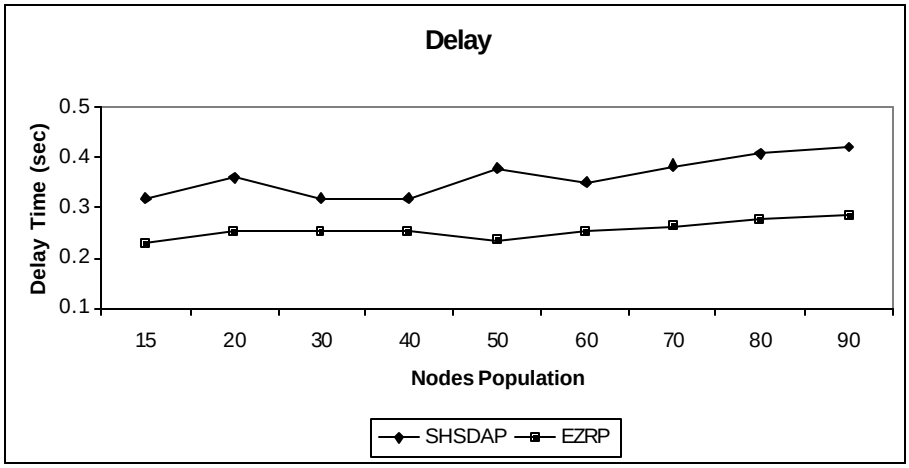


Fig. 10: Mean delay

The graph in Fig. 8 exhibits that adding SSD and SSA to the CBRP does not impose significant overhead on the network. Furthermore, for the sake of security we added some modules to the CBRP that increased the process time and the size of packet. Our results do not show any significant difference between either states. The overhead average for SHSDAP, CBRP and EZRO are 0.581, 0.552 and 0.547, respectively. This shows that our protocol is acceptable and because security is not considered in cases of CBRP and EZRP the minor increase in the overhead average in our protocol is well justified by the security added to the system.

Since all nodes in the MANETs are mobile and they move randomly. Some of they may go out the network and it is obvious that if owner of the resource have gone out the network the result of any request for that resource will be unsuccessful. In the next set of experiments, we tried to capture the ratio of the total number of successful SDs to the total number of SDs requests and estimate the total SD number of successful SDs from cache of each node. During simulation, the nodes request service instantly.

The graph in Fig. 9 shows that though hit ratios in both protocols are approximately equal, the average of success ratios of SD for SHSDAP is more than that of EZRP.

Figure 9 also shows that the increasing number of nodes in SHSDAP experiment does not have a considerable adverse effect on the hit ratio: success ratio is more than 86% for SHSDAP while success ratio for EZRP is around 78%. There are fixed number of services (15 nodes) which are randomly distributed among the nodes. Based on our experiment, the number of clusters increases in parallel with the number of nodes. Accordingly, it is obvious that hit rate on cache decreases with the increase in node population.

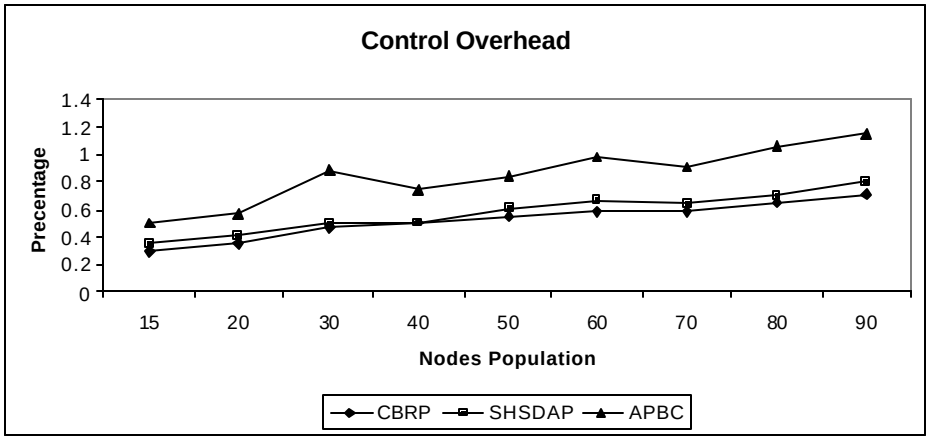


Fig. 11: Control overhead of CBRP, SHSDAP and APBC

In the next set of experiments, we tried to capture the distribution of mean delay for the discovery of every node. As explained earlier in the hit ratio experiment, the time spent on searching the cache, the time elapsed until a reply is received from the CH and the time elapsed until a reply is received from the other CHs in the SHSDAP is collectively called search time (delay). If the requested service exists in the cache node, it is considered as the best case and the delay is approximately zero. The worst case is when the request service is not available from the direct CH. When the service has to be provided by the other CHs the delay equals the collective time mentioned above. The calculated delay is shown in Fig. 10. To calculate the total delay, we captured the delay time for all nodes and all requests and then averaged the sum of delays in various states.

With respect to overheads incurred by security protocols, Fig. 10 shows that increasing the number of nodes in our experiment does not have a significant effect on the delay time, where the average delay for SHSDAP is about 1.4 times more than the average delay calculated for EZRP. This increased delay resulted from a delay caused by encrypting and decrypting information and security check. We believe that this delay is imposed by the security algorithms and is a necessary cost to implement secure transmissions in MANETs (whereas EZRP has no security mechanisms).

Comparison between SHSDAP, APBC and CBRP: Authentication Protocol Based on CBRP (APBC) is a protocol that detects and protects against malicious actions by three layer parties and peers in one particular ad hoc environment. As mentioned before, SHSDAP is a HSD and HSA which is secure against any malicious action in ad hoc environment. In our experiment, we intended to capture the effect of adding authentication to SHSDAP and APBC. Figure 11 shows the control message overheads versus number of nodes for Secure SD.

Table 3: Analysis of protocols (APBC, SHSDAP, CBRP, EZRP)

Protocol Item	CBRP	SHSDAP	APBC	EZRP
Service advertisement	o	Δ	o	Δ
Service discovery	o	Δ	o	Δ
Authentication	o	Δ	Δ	o
Efficiency	•/Δ	Δ	Δ	Δ
Safety	o	Δ	Δ	o
Scalability	•	•	•	•
Message overhead	•	•/Δ	o	•
Delay	•	•/Δ	o	•

o: Poor •: Normal Δ: Good

The graph in Fig. 11 indicates that the message overhead in the network is significantly less after adding SD, SA and authentication to the CBRP (SHSDAP) compared to when even authentication alone is added to CBRP (APBC). In Table 3 some other parameters of the all protocols are compared with each other.

Energy consumption comparison: Energy efficiency is another important issue for any protocol implementation in MANET. Some attributes such as sending and receiving data, idle and sleep state and discarding packet are important to addressed for energy consumption. Energy consumption in sending and receiving information is calculated using the following formula: [46]

$$\text{Energy} = M * \text{SIZE} + D \quad (1)$$

SIZE is the size of sending or receiving packet in byte. M and D are two constant parameters which are

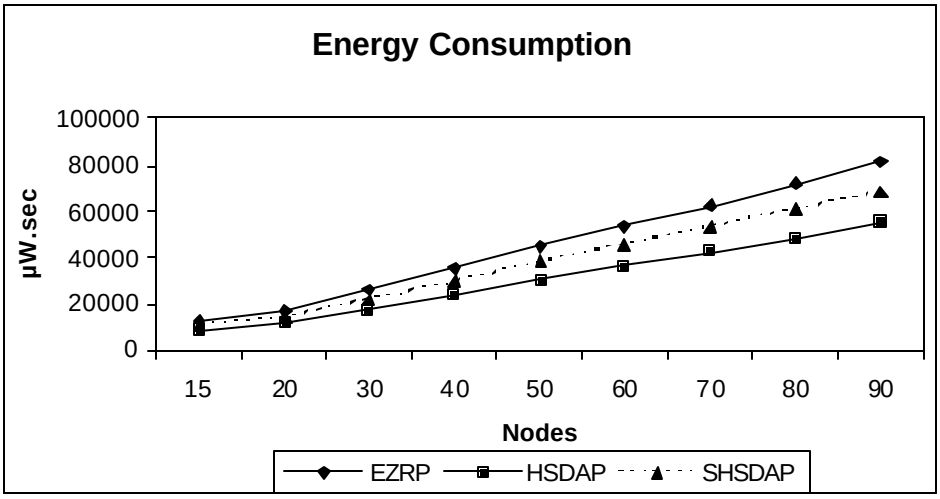


Fig. 12: Total energy consumption

Table 4: Power consumption measurements (Send & receive parameter) for LUCENT IEEE 802.11 2 MBPS

Parameter	M (µWsec/byte)	D (µWsec/byte)
Broadcast send	1.90	266
Broadcast receive	0.50	56

determined by hardware specification, protocol used and speeds of data transmission. Examples of energy consumption for idle and sleep states, the value of M and D for the LUCENT IEEE 802.11 2 MBPS WAVELAN PC CARD 2.4 GHZ are shown in Table 4. In this device, energy consumption for sending 1024 byte of data as a packet is calculated as follows:

Energy Consumption = 1.9 * 1024 + 266 = 2211.6 µW

In our experiment we considered a number of packets that were sent or received during SD. Based on the information in Table 4 we calculated the consumption for EZRP, SHSDAP and Hierarchical Service Discovery and Advertisement Protocol (HSDAP) Fig. 12.

Figure 12 clearly demonstrates that though energy consumption by EZRP while searching for a service is less than SHSDAP, simply because it does not have any security implemented, the overall energy consumption in our model is significantly less than EZRP.

Security performance analysis

- Unauthorized participation: Certificates, pair keys and CA public keys are given to every node through a complete supervision by CA. Moreover, inside each node is completely secure (with installed firewall) and all information between two nodes is securely transmitted. SHSDAP also only accepts participation of those packets that have been assigned with a certified key issued by a trusted authority. This prevents any unauthorized node from causing any harm to the network. CH/CA also supervises all communications and on the sight of the first evil deed of a node, its properties are added to the black list. Based on our algorithm, unauthorized nodes could not add any overhead to the network and could not do any forging.
- Spoofing: Since only the source node can sign its own private key and considering what was mentioned in part 1, nodes cannot spoof other nodes in any communication.
- Attacks: An Unauthorized node won't be able to start an effective connection and attack because: (i) it does not have any certificate to represent itself from the OO (CA); and (ii) it does not have the CA public key to decrypt the certificates. This not only prevents the connection of an unauthorized node to the other nodes, but it also prevents the unauthorized node from extracting or receiving other nodes' packets because they are encrypted by both offline CA key and the sender's key.

CONCLUSION

In this paper we propose a new DCA mechanism for MANETs. Based on DCA and RSA algorithms we introduced: SSA, SSD and SUS. We evaluated our protocol for its general security and routing performances, the influence of SDA on the network and energy consumption. Our experiments show that

SHSDAP performs well compared to the other protocols such as ABPC. The advantage of our protocol is in its implemented security that is overlooked in other available protocols.

SHSDAP is a good SSD protocol for ad-hoc networks since it has been implemented in routing layer which decreases message overhead In addition, it has employed a light weight security for SD and SA and a light weight security using service. As security is based on fully distributed certificate authentication, it decreases message and process overhead. The other advantage of SHSDAP for ad-hoc networks is that, it does not require central servers because it is based on CBRP. It is notable that it minimizes battery use in all devices. It also integrates a security model in order to guarantee the required security level by devices.

ACKNOWLEDGMENT

We would like to thank Universiti Sains Malaysia (USM) for the research grant and NAv6 Center for providing the research facilities in a collaborative environment.

REFERENCES

1. Dong, D.J., 2008. EE554: Special Topics on Ad Hoc Networks and Security Issues. Los Angeles: Dept. of Electrical and Computer Engineering California State University, Los Angeles.
2. Meshkova, E., J. Riihij?rvi, M. Petrova and P. M?h?nen, 2008. A survey on resource discovery mechanisms, peer-to-peer and service discovery frameworks. Article in Press in Computer Networks.
3. Gao, Z.-G., Y. Yang, J. Zhao, J. Cui and X. Li, 2006. Service Discovery Protocols for MANETs. MSN, pp: 232-243.
4. Abolhasan, M., T. Wysocki, E. Dutkiewicz, C. Liu and J. Kaiser, 2004. A review of routing protocols for mobile ad hoc networks. Ad hoc Networks, 2: 1-22.
5. Jiang, M., J. Li and Y.C. Tay, 1999. Cluster Based Routing Protocol(CBRP) (INTERNET-DRAFT draft-ietf-manet-cbrp-spec-01.txt). In National University of Singapore, I.E.T.F. (IETF), Ed., pp: 1-27.
6. Liu, C. and J. Kaiser, 2003. A Survey of Mobile Ad Hoc network Routing Protocols. Tech. Report Series, Nr. 2003-08.
7. Moghim, N., F. Hendessi, N. Movehhedinia and T.A. Gulliver, 2003. Ad-Hoc Wireless Network Routing Protocols and Improved AODV. In The Arabian Journal for Science and Engineering, 28: 99-114.
8. Cho, C. and D. Lee, 2005. Survey of Service Discovery Architectures for Mobile Ad hoc Networks. In Term paper, Mobile Computing, CEN 5531, Department of Computer and Information Science and Engineering (CICE) University of Florida.
9. Gr¨uninger, R., 2004. Service Provisioning in Mobile Ad hoc Networks. In Computer engineering and Networks Laboratory. Master Zurich: ETH Zurich.
10. Martínez, V.B., 2006. MOBILITY IN TCP/IP NETWORKS. In Ph.d CURSE Politechnic University of Catalunya (UPC).
11. Chakraborty, D., A. Joshi, Y. Yesha and T. Finin, 2002. GSD: A Novel Group-based Service Discovery Protocol for MANETS. In 4th IEEE Conference on Mobile and Wireless Communications Networks (MWCN 2002) Stockholm.
12. Schiele, G., C. Becker and K. Rothermel, 2004. Energy-Efficient Cluster-based Service Discovery for Ubiquitous Computing. In 11th ACM SIGOPS European Workshop Computine, Institute for Parallel and Distributed Systems (IPVS) Universität Stuttgart, Universitätsstr. 38, 70569 Stuttgart, Germany: acm.
13. Fan, Z. and E.G. Ho, 2005. Service Discovery in Mobile Ad Hoc Networks. In Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks. WoWMoM IEEE Explor, pp: 457-459.
14. Cheng, L. and I. Marsic, 2000. Service Discovery and Invocation for Mobile Ad Hoc Networked Appliances. In 2nd International Workshop on Networked Appliances (IWNA'2000) New Brunswick, New Jersey, USA.
15. Gerla, M., G. Pei, S.J. Lee and C.C. Chiang, 1998. On-Demand Multicast Routing Protocol (ODMRP) for mobile Ad-Hoc Networks. WAM Lab, UCLA.
16. Kozat, U.C. and L. Tassiulas, 2003. Network Layer Support for Service Discovery in Mobile Ad Hoc Networks. In IEEE INFOCOM 2003, pp: 423-434.
17. Ververidis, C.N. and G.C. Polyzos, 2005. Routing Layer Support for Service Discovery in Mobile Ad Hoc Networks. In Third IEEE International Conference on Pervasive Computing and Communications Workshops, pp: 258-262.
18. Zhu, F., M. Mutka and L. Ni, 2004. Prudent Exposure: A Private and User-centric Service Discovery Protocol. In Second IEEE International Conference on Pervasive Computing and Communications, PerCom'04, Orlando, Florida, USA, pp: 329-338.

19. Microsoft, 2000. Understanding Universal Plug and Play, White Paper.
20. Campo, C., C. García-Rubi, A.M. López and F.A. Mendoza, 2006. PDP: A lightweight discovery protocol for local-scope interactions in wireless ad hoc networks. Computer Networks, pp: 3264-3283.
21. Nidd, M., 2001. Service Discovery in DEAPspace. IEEE Personal Communications, 8: 39-45.
22. Microsystems, S., 2009. Jini Network Technology. In Jini Network Technology. S. Microsystems, Ed.: Sun Microsystems.
23. Guttman, E., C. Perkins, J. Veizades and M. Day, 1999. Ser-vice Location Protocol, Version 2 RFC 2608. In Network Working Group,Internet Society USA.
24. Sailhan, F. and V. Issarny, 2005. Scalable Service Discovery for MANET. In 3rd IEEE Int'l Conf. on Pervasive Computing and ommunications, pp: 235-244.
25. Lee, S., W. Su, J. Hsu, M. Gerla and R. Bagrodia, 2000. A performance comparison study of ad hoc wireless multicast protocols. Proc. IEEE Infocom, pp: 565-574.
26. Ge, R., D. Crescenzo, G. Fecko and S.M. Samtani, 2005. Efficient and secure indirect-address service discovery in MANET. In Military Communications Conference. MILCOM 2005. IEEE, pp: 1514-1520.
27. Yuan, Y. and W. Arbaugh, 2003. A Secure Service Discovery Protocol for MANET. In The 14th IEEE 2003 International Symposium on Persona1. lndoor and Mobile Radio Communication, pp: 502-506.
28. Hodes, T.D., S.E. Czerwinski, B.Y. Zhao, A.D. Joseph and R.H. Katz, 2002. An Architecture for Secure Wide-Area Service Discovery. Wireless Networks, 8: 213-230.
29. Zhu, F., M. Mutka and L. Ni, 2005. Facilitating secure ad hoc service discovery in public environments. In The Journal of Systems and Software Elsevier, pp: 45-54.
30. Arez, A. and F.C.C., 2003. A secure service discovery protocol for ad-hoc networks. In Workshop on Next Generation Networks-EUNICE 2003.
31. Scholten, H., V. Dijk, H.D. Cock, D. Preneel, B. D'Hooge and A.M. Kung, 2006. Secure Service Discovery in Home Networks. In Consumer Electronics. ICCE '06. 2006 Digest of Technical Papers. International Conference, pp: 115-116.
32. Ge, R., D. Crescenzo, G. Fecko and M. Samtani, 2005. Efficient and secure indirect-address service discovery in MANET. In Military Communications Conference, MILCOM 2005, IEEE, 3: 1514-1520.
33. Zhu, F., M.W. Mutka and L.M. Ni, 2003. Splendor: A Secure, Private and Location-Aware Service Discovery Protocol Supporting Mobile Services, PerCom 2003, pp: 235-242.
34. Zhou, H., M.W. Mutka and L.M. Ni, 2005. Multiple-key Cryptography-based Distributed Certificate Authority in Mobile Ad-hoc Networks, pp: 1681-1685.
35. Boukerche, A., 2002. Simulation-Based Performance Comparisone of Routing Protocols for Mobile Ad Hoc Networks. Simulation, 78: 7.
36. Perkins, C.E., E.M. Royer, S.R. Das and M.K. Marina, 2001. Performance comparison of two on-demand routing protocols for adhoc networks. Personal Communications, IEEE, 7: 13.
37. Haas, Z.J., M.R. Pearlman and P. Samar, 1997. The Zone Routing Protocol (ZRP) for Ad Hoc Networks. In Internet Draft, I. MANET, Ed., pp: 40.
38. Zhang, X. and L. Jacob, 2004. MZRP: An extension of the zone routing protocol for multicasting in MANETs. Journal of Information Science and Engineering, 20: 535-551.
39. Lee, K.-H., H.-S. Suh, S.-B. Han, S. Lee and C.-S. Hwang, 2004. An authentication protocol based on CBRP in ad hoc network. In The 6th International Conference on Advanced Communication Technology: IEEE Explorer, pp: 407-412.
40. Chiang, W.L.C.-C., H.-K. Wu and M. Gerla, 1997. Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. In IEEE SICON 97: IEEE.
41. Simons, G.J., 1979. Symmetric and Asymmetric Encryption. Computing Surveys, 11: 305-330.
42. Woo, T.Y.C. and S.S. Lam, 1992. Authentication for Distributed Systems. Computer, pp: 32-52.
43. Caporale, G.M., 1993. Symmetric versus Assymmetric Shocke in the EC. National Institute Economic Review, 144: 95-113.
44. WindowsITPro, 2006. Symmetric vs. Asymmetric Ciphers. In Vista and Longhorn Promise Enticing EFS Enhancements. 2009, Article, Ed.: WindowsITPro.
45. NS-2, 2008. Network simulator 2 (NS2), http://www.isi.edu/nsnam/ns/, In NS.
46. Feeney, L.M. and M. Nilsson, 2006. Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment. In INFOCOM 2001, pp: 1548-1557.