A Secured Dynamic Source Routing protocol for Mobile Ad Hoc Networks

بروتوكول توجيه مصدر ديناميكي مؤمن للشبكات المخصصة للجوال

Mazin Kadhum Hameed
Assist.lect
Babylon university/College of Information Technology / (Software Department)
Mazin_kadum2000@yahoo.com

Fryal Jassim Abd-Razak
Assist.lect
Babylon university/College of Information Technology / (Software Department)
Fryal.jassim@yahoo.com

Abstract

In the twentieth century at different times and in different places Communication technologies expanded. In the first the telephone invented as a wired technology and then as a wireless technology. In the later of the century computer communication has development. we can define the routing protocols as set of rules by which routers dynamically share their routing information.

Secured ad hoc routing protocols present a challenge, due to inherent characteristics of distributed cooperation, constrained capabilities of the nodes, open medium and dynamic topology. Due to such characteristics, these networks are highly susceptible to malicious attacks that may arise from several causes; non-deliberately when a node is damaged or deliberately when a node may need to save its resources, consume other node's resources, or isolate legitimate nodes from using the network. Most of the current ad hoc routing protocols are disrupted by malicious attacks. The most popular ad hoc routing protocol is the Dynamic Source Routing protocol(DSR) which is protocol finds the route when required dynamically and is on-demand source routing protocol. The DSR protocol contains two phases in its routing structure: route detection and route maintenance. To ensure the correct operations of DSR, provide security against malicious attacks is very important. This paper proposes a secured DSR; SecDSR which is protocol point -to- point certification of routing packets shared key between the two parties and using a Message Authentication Code (MAC) based on Ariadne protocol which relies on symmetric cryptography that is able to authenticate the source who initiated route discovery process to provide authentication. The tools and method that which used is it can used in conjunction with different mechanisms, one of which is TESLA (Timed Efficient Stream Loss tolerant Authentication) that setups shared secret keys beforehand. In this case time stamps are used to validate keysThe impact on performance caused by the use of such secured protocol is evaluated through simulation on NS-2. The DSR without security is first simulated. Then the secured version of the protocol; SecDSR is simulated. The analysis of simulation results revealed that secured ad hoc routing is achievable at the expense of increased routing overhead and end-to-end delay.

Keywords: Ad Hoc Routing protocols, DSR, performance Evaluation, Encryption

الخلاصة

إن تقنيات الاتصالات قد توسعت بشكل ملحوظ في أعوام مختلفة من القرن العشرين وفي اماكن مختلفة من العالم.ان اول هاتف ابتكر كان ضمن التقنية السلكية ثم تطور بعد ذلك الى التقنية اللاسلكية.اتصالات الحواسيب تطورت بشكل كبير في اواخر القرن.يمكن تعريف بروتوكولات التوجيه على انها مجموعة من القواعد التي من خلالها يمكن للموجهات ان تقوم بشكل

ديناميكي بمشاركة معلومات التوجيه الخاصة بها.ذلك وبسبب الخصائص المتأصلة للتعاون الموزع،قدرات العقد المقيدة،الوسائط المفتوحة و طوبولوجيا الديناميكية فان برتوكولات التوجيه المخصصه المؤمنة تشكل تحديا فعليا.كذلك وبسبب هذه الخصائص فان الشبكات تكون شديدة التعرض للهجمات الخبيثة والتي قد تنشا عن عدة اسباب قد تكون بعضها غير متعمد كتلف عقدة مثلا او قد تكون مقصودة ذلك عندما تقوم العقدة باستهلاك موارد عقدة اخرى عندما تحتاج الى حفظ مواردها او عزل العقدة الصحيحة من الشبكة وبسبب هذه الهجمات فان معظم بروتوكولات التوجيه تتعطل.يعتبر بروتوكول ال DSRمن اكثر بروتوكولات التوجيه اهمية اذ يعمل هذا البروتوكول على ايجاد المسار بشكل ديناميكي عند الحاجة وبروتوكول توجيه المصدر عند الحاجة.يحتوي هذا البروتوكول في بنيته على مرحلتين الاولى الكشف عن المسار والثانية صيانة المسار.ان من الاهمية القصوى ان يقوم هذا البروتوكول بعمله بشكل صحيح لتوفير الامن ضد الهجمات الخبيثة.في هذا البحث تم عمل DSR المؤمن الذي يعمل من نقطة الى نقطة اخرى بشهادة حزم التوجيه حسب مفتاح مشترك بين الطرفين وباستخدام رمز مصادقة الرسالة ذلك بالاعتماد على بروتوكول اريادن الذي يعتمد على التشفير المتماثل التي هي قادرة على مصادقة المصدر الذي بدأ عملية اكتشاف الطريق إلى توفير المصادقة.في هذا البحث تم استخدام ادوات وطرق مختلفة استخدمت جنبا الى جنب مع تقنيات مختلفة منها TESLA (موقوت كفاءة تيار خسارة المصادقة المتسامحة)والذي يقوم بتهيئة المفاتيح السرية المشتركة بشكل مسبق. وفي هذه الحالة تستخدم الطوابع الزمنية للتحقق من صحة المفاتيح حيث يتم تقييم الأداء من خلال التأثير الناجم عن استخدام البروتوكول المؤمن من خلال المحاكاة على NS2،حيث يتم اولا محاكاة DSR بدون اي امنية، ثم بعد ذلك النسخة المؤمنة من البروتوكول يتم محاكاتها. إن تحليل نتائج المحاكاة بينت أن التوجيه المخصص المؤمن يمكن تحقيقه ولكن يكون بزيادة النفقات العامة للموجه والتأخير من طرف إلى طرف.

1. Overview

Radio mobile nodes are assembling by network of mobile ad hoc dynamically produce a not permanent weave without the- method of existent mesh basic structure or centralized administration. The nodes are able to influence arbitrarily, changeful the network's topology quickly as a result unpredictably. As the radio row of extremely nodes is critically limited, the nodes commonly comply with their neighbors inside succession until extend the on the whole transmission range of the- network. In this networks, every node sending packages for other mobile nodes which may not be in the straight transmission range of each other, also it works not only as host, but further acts as a router. The assumption that routing protocols are depend on is that intermediary nodes will not alteration or drop the packets passed between nodes and all nodes will cooperate. To this assumption the dynamic and cooperative nature of network of mobile ad hoc presents substantial challenges. In a network of mobile ad hoc without node cooperation routes cannot be established, and packages cannot be sent. However, because any node could misbehave the cooperative behavior cannot be taken for granted, thereby forming a threat to the security of the exchanged packets between the mobile nodes [1], [2].

Individual nodes may not have any common interests and may not cooperate due to selfish behavior or malicious behavior. The non-cooperative behavior of selfish nodes is a result of fact that they want to, CPU cycles and memory save power. Wicked behavior is not mainly worried with power or any other savings but concerned in attacking and harmful the net by launching malicious attacks aiming to disrupt operation of routing protocols. Malicious nodes are defined here as nodes which cannot authenticate themselves as legitimate nodes because the lack of valid cryptographic information. There are two kinds of malicious attacks against network of mobile ad hoc: active and passive. The attacker in the active attacks, can upset the right works of a routing protocol by fabricating false information of router, by modifying router information, and by identity theft the other nodes [3], [4]. The attacker in the passive attacks not upset the routing protocol, it only tapping based on endeavors and packets of routing to extraction the significant facts such network topology and hierarchy of node from it. Especially if the nodes network of ad hoc obtain restricted materials such a that CPU processing capacity, memory and low battery power, protection of protocols of ad hoc routing it's difficult to design. A network of mobile ad hoc wireless has dual problem of security [5]. One, security of data that is sender on routes created via the routing protocols and the second is the routing protocols security, which let the nodes to associate with another. A routing protocol should implement a set of fundamentals to guarantee that the detect route from origin to target works rightly, to protect networks from malicious attacks. The main security problems result from the fact that routes are established with the help of intermediary nodes. It is therefore important that malicious nodes are to be avoided to update routing packets and only authorized nodes are allowed. Symmetric encryption is used to restrict malicious behavior of intermediate nodes [6], [7]. All routing packets between nodes are first encoded and then reply to the recipient nodes which share the keys to decrypt the routing packets and, if required, modify it according to the routing protocol specifications [8], [9]. The most popular ad hoc routing protocol is the DSR [10]. It is active routing protocol and usages a source routing system, which fitting that packet header include complete route for the packet. Routing information carried on the control information in the header of the DSR packets and nodes are supposed not to change this information. However, a malicious node can simply modify and fabricate fields of the routing packets. For this reason, authentication is essential to ensure legitimate access to the network. Without the proper authentication, no other security requirements like confidentiality, integrity and non-repudiation can be correctly implemented [11] as they rely on the accuracy of the authenticated protocol. This paper proposes a secured DSR named SecDSR based on Ariadne [12] that is depended on the authenticity and secrecy of keys that are stored at the nodes. It can used in conjunction with different mechanisms, one of which is TESLA (Timed Efficient Stream Loss tolerant Authentication) [13] that setups shared secret keys beforehand. In this case time stamps are used to validate keys. The impact on performance caued by the use of such secured protocol is evaluated though simulation on NS-2. The DSR without security is first simulated. Then the proposed secured version of the protocol; SecDSRis simulated and finally the influence of adding protection on the network efficiency is evaluated.

This paper is organized as the following. Section 2 shortly presents the dynamic source routing protocol. Section 3 summarizes the security attacks. Section 4 presents the proposed secured DSR. Section 5 briefly reviews the simulation environment, models, methodology, and performance metrics. In section 6, stimulant results and analysis are described with several figures to show the impact of adding security on performance of unsecured DSR. Lastly, section 7 presented conclusions and future work.

2. Dynamic Source Routing (DSR)

A DSR protocol finds the route when required dynamically and is on-demand source routing protocol[10]. The DSR protocol contains two phases in its routing structure: route detection and route maintenance. To decrease a cost of route detection, every node preserves a cache of source routes it has knowledgeable which it belligerently uses to restriction the occurrence and broadcast of route demand packets. Once a node wants a route to a target node and cannot take this route to that node then its route cache, it begins a route detection process with in the network, and the node is treated as the source node the detection [14]. The initiated node constitutes a route demand package (RREQ) by identifying the target node and a single identifier form the start node, at that moment transmissions the RREQ package to its adjacent, Each node receipt the RREQ, packages, and then rebroadcast the RREQ packet, if it has newly seen this demand by identifying the demand identifier from the start node, rejects the RREQ. Else, it attaches its specific address to the node list of the RREQ packages, and then re transmission the RREQ. When the RREQ reaches the end point, the destination node returns by uncasing a route response (RREQ) package backward the adjacent node which from it obtain the RREQ. A RREP package, which contains a duplicate of the collected list of nodes in the RREQ, is routed rear to the start node by reversing the RREQ path.

Route preservation is accepted every time there is a damaged link perceived in the specific route to the destination. Once the packages are progressive through an exact route, each node conducts the package to following the node in route and the next manner recognizes the package received. Once a damaged link is perceived in the target path the fragmented link will not recognize to the package transferred by the adjacent node, and the node conduct a route error package (RERR) to the start node. The initiated then replies to this ERR and ends sending the next packages and will look in its route cache for alternate routes and follow the next obtainable path. In paper, route caching will be inactivated for the objective to implement route authenticity [10].

3. Threats Analysis for DSR

DSR does not describe any safety machineries, which makes it weak to several menaces. These menaces contain packer fabrication and variation attacks. Meanwhile DSR describes no message validity tools, as opponent can for DSR RREQS RREPS or RERRs on behalf of other nodes. The controller information is the heading of the DSR packages transmits the routing information and nodes are supposed not to alteration this information. Nevertheless, a wicked node can simply impersonate or fabricate the routing packets. In impersonation, malicious node imagines to be alternative node when it know is IP or MAC address and modifications it to its specific MAC or IP address. In forgery, malicious node generates false route packets. In rushing attack [15], when wicked node obtains the route demand, it responses with a route response package backward to the source and allegation itself as having new sufficient route to the end point no problem even if it recognizes the route or not, this fake route reply introduces malicious node as a real destination and becomes a member of the active route. The source receipt the route response package from the wicked node may fix that the route over wicked node is the new route to the goal and start to transfer date packages beside the route through wicked node. As a result, when a malicious node is selected on a path, it can take further actions to maliciously disrupt function of the protocol. In black hole attack [16], it deletes data packages completely, while in gray hole attack [17], a malicious node may delete any route request packets, or route reply, or route error packets. Additional attack is the route cache harming attack, in which every node can spy the transport, and if it discoveries route information it loads it to its cache for later use. A wicked node can then send out the cheat bundles across itself. Then, adjacent nodes catch this and load the route to its own cache [18]. The invisible-node attach is another attach in which a malicious nodes deny as the goal node in the connection with the initiator and as the initiator in the connection with the destination. The majority of existing routing protocols are disrupted by these attacks [19]. Therefore, it is important to develop a security mechanism that can prevent malicious attacks.

The current cryptographic security solution can be broadly divided into categories: asymmetric and symmetric cryptographic systems [20]. Bothe needs the presence of an online confident third part,. The nodes of mobile are restricted in availability of power, memory, computing resources, and communications bandwidth. Therefore it impossible to use asymmetric algorithms for principal managing. This algorithms are very arithmetically compact and, therefore, intensive force because they include the modulus processes and exponential of huge numbers. Thus, the general method is to use symmetric key encryption where the last points of the connection share a secret key. They are three to four commands of scale faster to compute, but they are not useful as public key encryption methods, which complicate the design of the protocol. Therefore, the proposed secured DSR will be based on symmetric cryptography to provide authentication during route discovery, establishment and maintenance which is described in the following section in detail.

4. The Secured Dynamic Source Routing; SecDSR Protocol

A shared key between the two pieces and a Message Authentication Code (MAC) are both using in the SecDSR protocol which is point -to- point authentication of routing packets. Whereas, for authentication of a broadcast package such as RREQ we used a Time Efficient Stream Loss-tolerant Authentication(TESLA) broadcast authentication protocol. In TESLA a one way key sequence is generating by the sender and in agreement with which it discloses the keys of the sequence it defines a schedule in reversal order from generation. All nodes loosely time synchronized with each other with fixed synchronization error is assumed. Additional, in the network every node is assumed to strongly distribute the authentication commitments to each other node and at initialization that TESLA key commitment are established with neighbors.

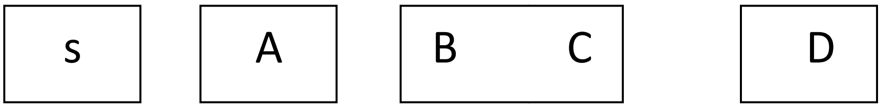
The protocol works as indicated in the figure in and its security analysis is proved in it works as follows. When a node transfers a route demand it contains its owned address, source or initiator "s", the address of the target or end node "D", a digit "id" that the initiator sets and which has not been used recently in initiating the a route detection, a TESSLA *time period* "it" that represent the

Pessimist predictable arrival time of the RREQ to the target. Then the source of the RREQ initializes the hash chain (ho) to MACk (S, D, id, it), this indicate a Message Authentication Code (MAC) calculated with key k over single data where k is a symmetric key with source and destination. Route request packet contains eight fields as follows:

<REQUEST, source, target, id, ti, hash chain, node list, MAC list>
Since MAC list and node list is blank in this stage, the RREQ, package appearances as follows:
<REQUEST, S, D, id, it, ho, 0.0>
When an intermediary node (A) obtains RREQ, which is not the destination, its checkup its resident table of ‹ originator, id› value from current RREQ, it, has acknowledged to check if it now detect a RREQ the node rejects the package. Furthermore, the node checkup incase the time period in the RREQ, is legal. A legal time period is one that it is not very distant in the future and its equivalent key should not be revealed so far yet. The package with illegal time period is ignored. Else, the existing node add its address into the node list, exchanges the hash sequence by a new one containing of its address in addition to the old one "h,=H(A, ho)", and adds a MAC to the whole package to the list of MAC. The MAC is computed by the TESL A index k' where k' is a TESL A index of intermediate node A, and I is the key for the time period indicated in the RREQ. Consequently, M_A is defined as following:
M_A= MAC k(REQUEST, S, D, id, ti, hO , (A), 0)
Lastly, the node rebroadcast the changed RREQ to its adjacent. The target node checkup the legitimacy of the route demand upon receipt it. A route demand is considered legal if the keys from the indicated time period have never revealed, and if the embedded hash sequence can be verified. Consequently, the destination node (D) receiving the RREQ checkup legitimacy of RREQ by defining keys from indicated time period that not yet revealed and the field of hash sequence is equivalent to the following:
H (nas,is H(…,H(nis MACK(S, id, ti)…)))
Where n is a amount of nodes in the mode list and ni is a node address of location i of list of node in RREQ. Once the target node fixes the RREQ is legal, it yields a RREP to the originator (S), holding the following eight fields:
<REPLY, destination, source, time period , list of node, list of MAC, destination MAC, key list>
Then the destination produces and transmissions a route answer package for every legal route demand it obtains. A route reaction holds the identical fields with the equivalent route demand, and furthermore it holds a destination MAC field and an blank key. The destination field of MAC given to compute the MAC of previous field of the route reaction and key the destination share with the initiator.
because key list is empty in this case, RREP packet appearance as
<REPLY, D, S, it, (A), (MA), MD, o>
The reaction is advanced rear to the originator by following the opposite of the route embedded in the list of node, as indicated by the DSR protocol. An intermediary node that accepts the route reaction delays till the indicated time interim permits it to release its key, which it adds to list of the key and forward the communication to the following node. Upon receipt a route reaction, the originator validates the legitimacy of every key in key list, of the destination MAC in the list of the MAC. Node sending PRWO delays till it is capable to reveal its own key from indicated time interim; then it adds the field of the key list in the REPLY to its key from that time interim and forward the package depend on to originator route specified in package. The route reaction package appearances as follows:
<REPLY, D, S, ti, (A), (MA), MD,(K')>
Lastly, after the originator obtains a RBEP, it validates every key in list of the key it legal, destination MAC legal, and every MAC in list of MAC is legal. Whenever each these toys succeed, the node takes the RREP. The SecDSR protocol also protect rout maintenance, which guarantees the legitimacy of route error packages about fragmented links in the network of the ad hoc. A node that produces a route error contains TESLA authentication parts in the package. Consequently,

every node that frontwards the route error towards the destination is able to validating it. The intermediary nodes buffer the route error package and its validation does not happen till the node that produced it releases the key.

Figure 1 illustrate an example of route detection in the proposed SeeDSR.



S: ho=MACksD=(REQUEST), S. D, id, in

S → * *(REQUEST, S. D, id, in, if, ho, o.o)*

A: *h1 = H {A, ho}*

Ms = MACkA (REQUEST. S.D. id . ti h. (A) . o)

A → * (REQUEST.*S. D. ID. TI. H1*. (A). (MA)

B: *h2= H1 (B. h1)*

MBB=MAC kB (REQUEST. S. D. id, h2. (A . B).(MA)

B *→ (REQUEST.*S. D. I d. it .h2* . (A**). (MA.** ***M2)***

C: *h3 = H(C. h2* ***)***

MC = MAC.KC (REQUEST. S.D Id .it h3 . A .B. C1 (MA..M8

C → * (REQUEST.*S. D. ID. ti. h2*. (A. B .C). (MA . Mk. Mc)

D: MD= MAC kDS (REPLY. D. S.it h)

D→ C: (REPLY. D. S. it .(A. B . C) . MA . Ma . Mc) Ma . D)

C→B (REPLY. D. S. it .(A. B . C) . MA . Ma . Mc) Ma kD. Kca))

B→ A REPLY. D. S. it .(A. B . C) . MA . Ma . Mc) Ma Kc .kDa))

A→ s : REPLY. D. S. it .(A. B . C) . MA . Ma . Mc) Ma KB .kAs))

Figure 1 example of route detection in the proposed SeeDSR.

The originator nods *S* is attempt to fix a route to a destination node *D.* The font apparent line specifies altered information fields, relatively the preceding information of that type.

5. Simulation Environment

All nodes are synchronized loosely time with each with fixed synchronization errors. Additional, every node is assumed to safely dis- tribute obligations to each other node in the net and those TESLA obligations are well-established with adjacent. Network Simulator NS-2-31- allinone package [21] is used to implement the unsecured DSR and SecDSR and to analyzed the effect of adding security on achievements. The simulation integrated common technological values specifications of IEEE 802, 11b wireless net with network parameters chosen such that real communication environment is depicted more accurately. The simulation is performed under window operating system using Cygwin Modifications to the current release were done to incorporate the SecDSR as a new protocol using C++ code [22].The mobility scenario files and communication scenario files are created and Simulated. A code of Tool Command Language (TCL), it is written to prepare wireless simulated elements.To produce trace files that contain a list of all most important events such as package transmitted, packet received, packet dropped, type of packet source, and destination during a simulate it requires that the TCL script is compiled and run. The tracking data is store in as yield file for post-processing. These files are parsed by AWK, in order to get information needed to assess achievement measures. The yield is conspired using Excel to graphically concentration the performance measures.

5.1Simulation Methodology

In the simulation, mobile nodes randomly move in the flat square of 1500 by 300 meters, and the duration of the simulation is 900 seconds. The network density is varied from 10 to 60 nodes in a step of 10. Every run of the simulation is accepted as input, the status file that specifies the exactly mobility for every node the exactly arrangement of packages initiated by every node. This regenerated scenario files ensure that the two versions of the routing protocol run under same environmental conditions. There are an overall 20 pairs of interconnecting nodes, with every source transfer out stable bit rate (CBR) traffic movement with package size of 64 bytes at a rate of 4 packages/second. The biggest from finale to finale net wait is 0.2 second. The MAC size, hash size and key size are agreed to 80 bits. The TESLA time wait is set to 2 second, and the synchronization error is get to 0.1 second as summarized in Table 1. Every data point is serving as an average of ten randomly generated scenarios, where seed of each run is varied to influence placement and mobility of nodes. The DSR protocol is first simulated on NS.2 and then the SecDSR is implemented as a protocol independent module [23]. The SecDSRis duplicated in Ns-2 directory under name SecDSR. All files in that directory are changed and the protocol is integrated to the NS-2 simulator. The performance metrics for both DSR and seeDSR are evaluate d and then the effect of adding security on the performance metrics aanalyed[24],[25].

Table l Ns-3 Simulation Parameters

Simulator	Ns-231
Examined Protocol	DSR, SecDSR
Simulation Duration	900 seconds
Simulation Area	1500 m×300m
Propagation model	Two Ray Ground Reflection
Link Bandwidth	2Mbps
Transmission range	259 meter
First Route demand break	2seconds
Highest Route demand break	40 seconds
Cache Size	32 routes
Mobility model	Random Way point
Maximum Speed	10 meter per second
Pause time	10 seconds
Amount of links	20 CBR
Data load	64 bytes
package Rate	4 packets per second
TESL Time Period	2 second
Pessimistic End to end broadcast time	02 second
Highest Time Synchronization Error	0.1second
Hash Length	80 bits

In table 1 simulation duration, simulation area, propagation model, link bandwidth and transmission range represent scenario parameters whereas first route demand break, highest route demand break and maximum route request timeout represent DSR parameters, however pessimistic end to end propagation time ,TESL time period , hash length, highest time synchronization error represent TESLA parameters.

5.2 Performance Metrics

The performance is evaluated under the same movement models and communication models using the following basic metrics are used to gather information about the natural or unsecured DSR and secured DSR routing protocols, with equations provided in the following [26].

a) package Delivery Ratio(PDR)

PDR is the ratio among the numbers of data packages accepted from application layer of target nodes to the number of packages that transfer from application layer of initiator nodes.
Also, it represents the efficiency of the protocol in sending data packets to their destination.

PDR=Number of Successfully Delivered Packets/ Total Number of Transmitted Packets (1)

b) Average end to end Delay

This metric provides the average time in seconds occupied from a data packages to reach their relevant targets.

C) Routing Package Overhead Is a rate among the overall control packages numbers produced to the overall number of data packages established throughout the time of simulate. All hop-wise communication of a controller package counts as one communication. The over-all number of control packages is computed by number of route replies, route requests, and route errors of each protocol. It is used to examine communication overhead caused by secured protocol.

RPO=Total Number of Routing Packets/ Total Number of Transmitted Packets (2)

6. Simulation Results and Analysis

A results of simulation revealed that SecDSR outperforms unsecured DSR in details of package delivery rate. The Table2 and figure 2 show the different between the proposed SecDsr and Dsr.However, SecDSR increases routing overheads as result of the adding of the hash value on every authentication which caused the increase in size of each packet. This increased overhead causes some congestion in the network and consequently growths end-to-end wait. At higher network sizes, SecDSR exhibits higher delay than DSR due to the increased overhead which it decreased available network capacity. Three basic metrics are used to evaluate performance of non secured and secured routing protocols are analyzed as follows.

6.1 Packet Delivery Ratio

The unsecured DSR and SecDSR protocols exhibited similar behavior with respect to package delivery ratio. The package delivery ratio is not greatly affected with additional overheads of encryption, throughout route discovery and maintenance process. As SecDSR uses authentication with shared keys between nodes, it takes more time for route discovery and once secure routes are discovered the delivery ratio increases gradually because of the secure route. Once routes are discovered, the SecDSR protocol presented a slightly upper PDR in relation to the unsecured DSR. As network size increment. SecDSR presented a similar delivery ratio, as both protocols operate under attack-free environment. In average, the two protocols gives a linear increment in packet delivery ratio as number of nodes increase up to 30 nodes, and then they decrease gradually due to network congestion.

6.2 End to end Delay

Is observed that DSR showed a better performance than SecDSR protocol. The key issue for the low performance of secured protocol is the important increment in time for authentication of packets in every intermediary node that compose route till the destination. Where, delay increases when a number of nodes increased.

6.3 Routing Overhead

The efficiency of SecDSR is decreases whenever increase in number of nodes, because it is a source routing protocol and the rise in the number of nodes causes a important growth in routing overhead due the validation of packets is each intermediary node that comprise route until the destination.

Table2 the different between SecDsr and UnsecuredDsr

Secured DSR	**Unsecured DSR**
1. Based on symmetric cryptography to provide authentication during route discovery. 2. Presented a slightly higher PDR. 3. Increased end-to-end delay since the additional overheads of encryption. 4. Increased routing overhead since the additional overheads of encryption. 5. More security.	1. Not based on symmetric cryptography. 2. Presented less PDR. 3. Decreased end-to-end delay since have not additional overheads of encryption. 4. Decreased routing overhead since have not additional overheads of encryption. 5. Less security.

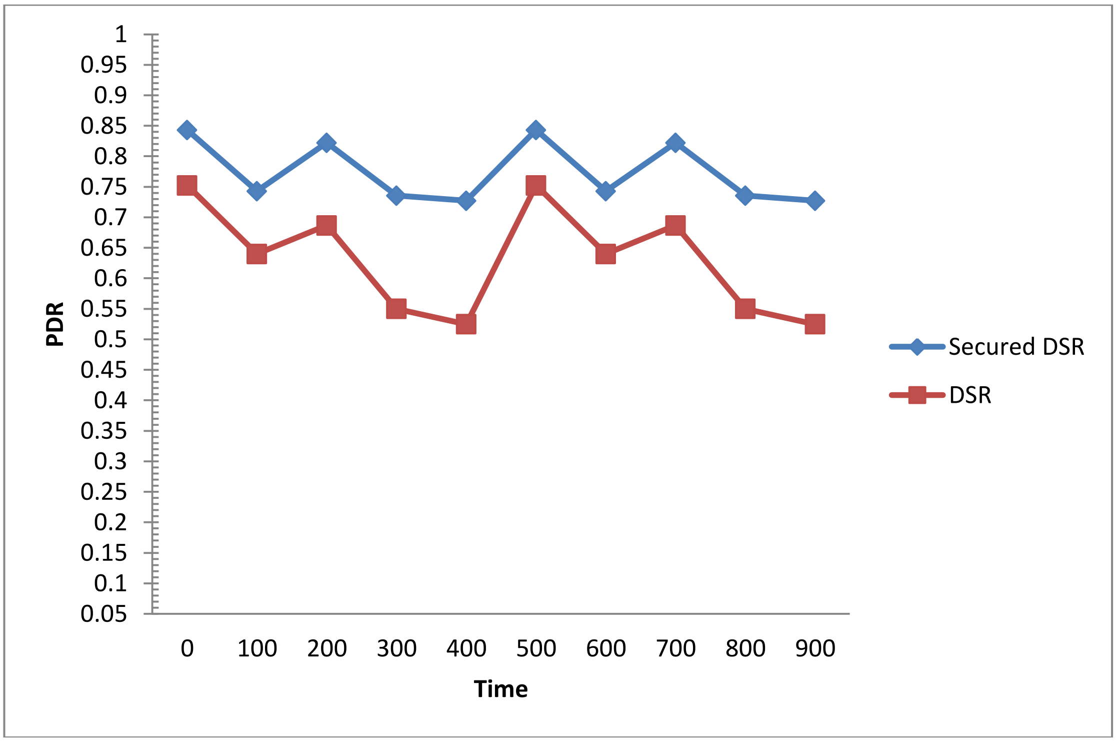


Figure2 the PDR for SecDsr and Dsr

7. Conclusion and Future Work

We are confirmed from the analysis and simulation that the influence due to the adding of security mechanism was high. Using of security protocol will be implicated in greater values for end-to-end wait and routing overhead metrics. Therefore, the usage or lack security routing protocols will be directly relevant by the reason for which the ad hoc wireless network will be used and by the predictable values for the performance metrics. Finally, the prove of security improvement is outer the domain of this paper and additional effort is required to a proper model based on hard mathematic grounds that can exactly offer a description for secured ad hoc routing and to properly verify if a proposed protocol satisfy the description under assured assumptions.

8. References

[1] JaydipSen, Piyali Roy Chowdhury, and IndranilSengupta, an analysis of Routing Distruption Attack on DSR in Ad Hoc Wireless Networks. International Conference on Next Generation Communication Systems, ICONGENCOM, pp. 257 -267, 2003.

[2] BounpadithKannavong, HidehisaNakayams, Yoshiaki Nemoto, Abbas Ja,a;o[pir. AndNei Kato, "A sirverypfRpitongAttacls in Meblie Ad Hoe Networks" LEEEWireless Communications. 2007.

[3] GergelyAcs :LeventeButtyan, and Istvanvajda, Provably Secure On Demmand Source Routing in mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, vol.5, No.11. 2006.

[4] P.Papadimitratos, Z. Haas. P Samar. The Secure routing protocol for ad hoc networks, Proceedings of the 2nd ACM workshop on wireless security, USA. Pp. 41 -50, 2003.

[5] Md. Liakat Ali, Security Threats in mobile Ad Hoc, vol.14, No.4, 255-265, 2006.

[6] Kamanshis Biswas and Md, Liskat Ali "Security Threats in Mobile Ad hoc Network" Master Thesis, Bickinge Institute of Technology, Sweden, 2007.

[7] Yih Chun Hu,"ASurvey of Secure Wireless Ad Hoc Routing" IEEE security and privacy,pp,28-36, 2004

[8] Rui Yang, Qi Xia, Qun Pan, Wei Wang, and Ming Li, "New Fnhancement Scheme for Secure Routing Protocol in Mobile Ad Hoe Networks", Proceeding of the Fifth international conference on Computer and information Technology. 2005.

[9] PatrokiosArgroudis, and DonalO'Mahony, "Secure Routing For Mobile Ad Hoc Networks, IEEE Communications Surveys and Tutorials,2005.

[10] D.B Johnson, D.A Maitz, and Y Hu, Dynamic Source Reuting Protocol for Mobile Ad Hos Networks, (DSR),"IETF MANET, interment Draft, 2003.

[11] S. Marti,. T. Giuli, k. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" Proceeding of Sixth Annual International Conference Mobile computing and Networking (Mabicom), pp. 255-265, 2000.

[12] Y.C Hu, A. Perring, and D.B Johnson, "Ariadne: A Secure On Demand Routing Protcol for Ad hoe Networks", Procoeding of Eighth Annual International Conference, Mobile Computing and Networking)Mobicom), pp, 1-23,2002.

[13] Adrian Perrig, Ran Canetti, J.D, Tygar, and Dawn Song, Efficient Authentication and signing of Multicast Streams Over Lossy Channels, IEEE Symposium on Security and Privacy, Pages 56 – 73, May 2000,

[14] Su Mon Ba, Hannan Xiao, AderemlAderect ,Jammes Malcolm, and Bruce Christianson, 'A Performance Comparison of Wireless Ad Hoc Network Routing Protocols Under Security Attack", IEEE computer Society, 2007.

[15] Yih-Chun Hu, AdtianPerrig, and Dave Johnson, "Rushing Attacks and Defense workshop on Wireless Security (WiSe), San Diego, California , September 2003.

[16] Baruch Awerbuch, Reza Curtmola,David Holmer,and Heret Rubes,ODSBR:An On Demand Secure Byzantine Resilient Routing Proctocol for Wireless Ad Hoc Networksmm ACM Journal, 2007.

[17] ShahulAhamed Ali Mohammed, "Evaluation of Mobile Ad heeSecur Routing Royal Institule of Technology, Sweden, 2006

[18] N. Bhalaji. "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", Journal of Software, Vol. 4, NO. 6, pp 536-543, Academy Publisher, 2009

[19]P.Lakshmi Ramana, Secured VRP for MANET's in Presence of Malicious Nodes, MSC Thesis, Computer Science and Engineering department, National Institute of Technology Roukela, India, 2009.

[20] DiaaSalama Abdul Elminaam, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmeric Encryption Algorithms"ijCSNSIntemational journal of Computer Seience and Network Applications Protocols, and Services 2008.

[21] The Network Simulator –Ns-2 home page, Available at http:/www.isi. edu/nsnam/ns.

[22] The Monarch Project home page. Available a t http://www.monarch.es.ricreda.

[23] Francisco Ros, and Pedro Ruiz, Implementing a New Unicast Routing Protocol in NS2, Master Thesis, Murcia University, 2004.

[24] Sheenusharma, and Roopam Gupta, "Simulation Study of Blackhole Attach in the Mobile Ad Hoc Networks", international Conference on Network Applications,Protocols, and Services, 2008.

[25] SemithDokurer,'Simulation of Blackhole Attack in Wireless Ad Hoe Networks".Master Thesis. Atihm University. 2006.

[26] Shan Gong, "Quality of Service Aware Routing Protocols for Mobile Ad Hoc Networks", Master Thesis, Helsinki University of Technology, 2006