MAODV: A Defense against Sybil Attacks in Wireless Networks

Manish Kumar Suman
CSE department, NIIST Bhopal

Sini Shibu
CSE department NIIST, Bhopal

ABSTRACT

Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. An ad-hoc wireless network is a collection of nodes that come together to dynamically create a network, with no fixed infrastructure or centralized administration. In mobile ad-hoc networks, data transmission is performed within an untrusted wireless environment. The lack of centralized infrastructure in ad-hoc network makes it vulnerable to various attacks. Sybil attack is one of the serious attacks, which form a serious threat in the networks, especially against many ad hoc wireless routing protocols, and location based wireless security system.

In the Sybil attack incorporates a malicious device with the ability to illegitimately take on several identities in the same network. The forged identity from a malicious device is called a Sybil node. A malicious device can obtain an identity for a Sybil node in two different ways; (a) generating a new identity; or (b) taking the identity from an existing node (with the cooperation of the node or by developing a spoofing attack). We identify two types of Sybil attacks. In the first type, malicious nodes do not take part in finding routes, meaning that, legitimate nodes do not know their existence. In the second type, malicious nodes do create route advertisements and legitimate nodes are aware of the existence of malicious nodes, just do not know they are malicious. Some of the researchers have proposed many solutions for Sybil attack.

In this paper, an efficient method to detect a Sybil attack called modified Sybil detection AODV protocol has been proposed. Detection of Sybil attack is performed using number of hops in different paths from source to destination and delay of each node in different paths from source to destination. The destination is able to detect both kinds of Sybil attacks. The performance of modified Sybil detection AODV protocol is justified by simulations.

Keywords

Ad-hoc networks, Security, Sybil attack, Attacked path, Wireless.

1. INTRODUCTION

In many remote systems administration situations in profitable utilize today the clients' gadgets convey either by means of some organizing foundation as base stations and a spine system, or specifically with their proposed correspondence accomplice, e.g. utilizing 802.11 as a part of specially appointed systems [1]. Fig.1 shows the systems and parts inside of the Base based Wireless Networks.

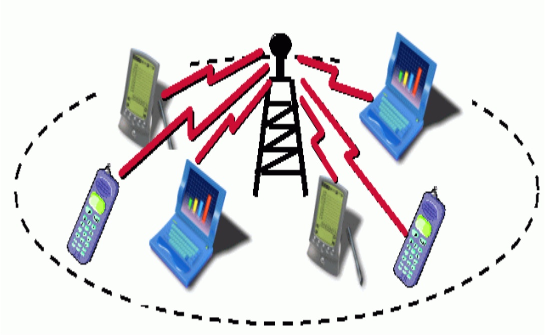

Fig 1: Infrastructure-based Wireless Networks

Interestingly a portable impromptu system (MANET) is a self-designing system that is framed naturally by means of remote connections by an accumulation of portable hubs without the assistance of a settled framework or unified administration. Each hub in portable specially appointed systems is furnished with a remote transmitter and recipient, which permit it to correspond with different hubs in its radio correspondence range [2]. Hubs normally have the same physical media; they transmit and secure signs at the same recurrence band, and take after the same bouncing grouping or spreading code [3]. In the event that the destination hub is not inside of the transmission scope of the source hub, the source hub takes help of the middle of the road hubs to speak with the destination hub by handing-off the messages bounce by jump. Fig.2 showed the Mobile impromptu system. All together for a hub to forward a bundle to a hub that is out of its radio range, the collaboration of different hubs in the system is required; this is known as multi-bounce correspondence. Thusly, every hub must go about as both a host and a switch at the same time.

While the security prerequisites for impromptu systems are the same the ones for settled systems, in particular accessibility, privacy, honesty, confirmation, and non-disavowal [4] versatile remote systems are for the most part more powerless against data and physical security dangers than altered wired systems [5]. Securing remote impromptu systems is especially troublesome for some reasons including helplessness of channels and hubs, nonappearance of framework, powerfully changing topology and so on [6]. The remote channel is open to both honest to goodness system clients and malignant aggressors. The theoretical of brought together administration makes the established security arrangements in light of affirmation powers what's more, on-line servers inapplicable. A noxious aggressor can promptly turn into a switch and upset system operations by purposefully ignoring the convention details.

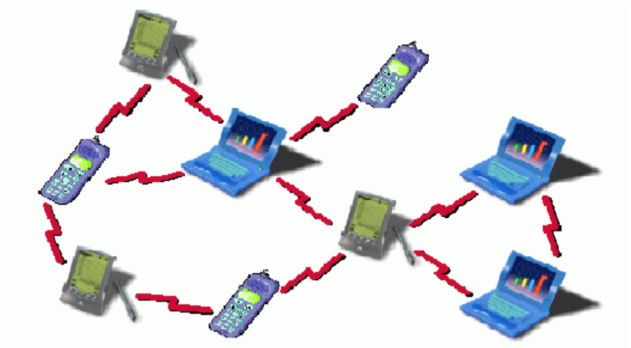

Fig 2: Mobile specially appointed systems

The hubs can move arbitrarily and unreservedly in any course also, compose themselves discretionarily. They can join or leave the system whenever [7]. The system topology changes oftentimes, quickly and capriciously which essentially changes the status of trust among hubs and includes the unpredictability to steering among the portable hubs. The self-centeredness that hubs in specially appointed systems may have a tendency to deny giving administrations to the event of different hubs keeping in mind the end goal to spare their own assets (e.g., battery force) presents new security issues that are not address in the base based systems.

The rest of the paper is organized as follows: section 2 presents several secure attacks. Section 3 presents the popular secure protocols in ad hoc networks. In Section 4 conclusion is presented.

2. SECURITY ATTACKS

Securing remote specially appointed systems is a very difficult issue. Because of element circulated framework less nature what's more, absence of unified observing focuses, the specially appointed systems are powerless against different sorts of assaults. Impromptu systems need to adapt to the same sorts of vulnerabilities as their wired partners, and additionally with new vulnerabilities particular to the specially appointed connection [8]. Moreover, customary vulnerabilities are likewise emphasized by the impromptu worldview. Firstly, the remote channel is available to both genuine system clients and noxious aggressors. The impromptu systems are helpless to assaults going from inactive listening in to dynamic meddling. Also, the absence of an online CA or Trusted Third Party adds the trouble to send security components. Thirdly, cell phones have a tendency to have restricted power utilization and calculation abilities which make it more helpless against Denial of Service assaults and unable to execute calculation overwhelming calculations like open key calculations. Fourthly, in MANETs, there are more probabilities for trusted hub being bargained and after that being utilized by foe to dispatch assaults on systems; at long last, hub versatility and incessant topology changes implement continuous organizing reconfiguration which makes more risks for assaults, for instance, it is hard to recognize stale steering data and faked directing data [9].

Specially appointed systems assaults can be delegated detached or dynamic [10]. Aloof assault implies that the aggressor does not send any message, however just listens to the channel. Latent assaults don't disturb the operation of a convention, yet just endeavors to find significant data. Dynamic assaults might either being coordinated to disturb the typical operation of a particular hub or focus on the execution of the specially appointed system all in all.

For inactive assaults, the assailant listens to the channel and bundles containing mystery data (e.g., IP addresses, area of hubs, and so on.) may be listened stealthily, which abuses privacy. In a remote domain it is more often than not difficult to recognize this assault, as it doesn't deliver any new activity in the system.

Dynamic assaults, including infusing bundles to invalid destinations into the system, erasing bundles, adjusting the substance of bundles, and imitating different hubs damage accessibility, honesty, validation, and non-revocation. Not at all like the aloof assaults, dynamic assaults can be identified and in the end maintained a strategic distance from by the true blue hubs that partake in a specially appointed system [11].

Certain dynamic assaults can be effortlessly performed against a notice hoc system. Understanding conceivable type of assaults is continuously the initial move towards growing great security arrangements. In view of this risk examination and the distinguished capacities of the potential assailants, a few surely understood assaults that can focus on the operation of a steering convention in an specially appointed system are examined.

• Impersonation. In this kind of assault, hubs may be capable to join the system imperceptible or send false steering data, taking on the appearance of some other trusted hub.

• Routing Table Overflow. In a steering table flood assault the vindictive hub surges the system with false course creation parcels to non-existing hubs to overpower the steering convention usage keeping in mind the end goal to devour the assets of the partaking hubs and upset the foundation of authentic courses. The objective is to make enough courses to keep new courses from being made or to overpower the convention usage. Proactive steering conventions are more defenseless against this assault, since they endeavor to make and keep up courses to every single conceivable destination. A vindictive hub to execute this assault can basically send unreasonable course promotions to the system. To actualize this assault keeping in mind the end goal to focus on a responsive convention as is AODV somewhat more entangled since two hubs are required. The in the first place hub ought to make a true blue solicitation for a course and the malevolent hub ought to answer with a produced address [12].

• Sleep Depravation. The lack of sleep torment goes for the utilization of asset of a particular hub by continually keeping it occupied with directing choices [13]. This assault surges the system with directing activity keeping in mind the end goal to expend battery life from the hubs and accessible data transfer capacity from the impromptu system. The malevolent hub ceaselessly asks for either existing or non-existing destinations drives the neighboring hubs to handle and forward these parcels and consequently expend batteries and system transfer speed blocking the ordinary operation of the system.

• Location revelation. Area exposure is an assault that focuses on the security prerequisites of a specially appointed system. Through the utilization of movement investigation systems [14] or with less complex examining and observing methodologies an aggressor is capable to find the area of a hub, and the structure of the system. On the off chance that the areas of a percentage of the go-between hubs are known, one can pick up data about the area of the destination hub too.

• Routing table harming. Steering conventions keep up tables which hold data with respect to courses of the system. In harming assaults the malignant hubs create and send created activity, or alter true blue messages from other hubs, with a specific end goal to make false sections in the tables of the taking an interest hubs [15]. Another plausibility is infusing a RREQ bundle with a high grouping number; this will bring about that all other genuine RREQ bundles with lower succession number will be erased [16]. Directing table harming assaults can bring about choice of non-ideal courses, production of directing circles, bottlenecks and notwithstanding dividing certain parts of the system.

• Black Hole [17]. A pernicious hub utilizes the directing convention to infuse false course answers to the course asks for it gets promoting itself as having the briefest way to a destination whose parcels it needs to capture. Once the manufactured course has been set up the malevolent hub can turned into an individual from the dynamic course and capture the correspondence parcels. System activity is occupied through the noxious hub for listening in, or pull in all activity to it keeping in mind the end goal to perform a dropping so as to foreswear of administration assault the gotten parcels or the initial step to a man-in-the-center assault.

• Wormhole. The wormhole assault includes the participation between two assailants [18]. One aggressor catches steering movement at one purpose of the system and passages them to another point in the system that shares a private correspondence join between the assailants, then specifically infuses passage activity over into the system. The two conspiring assailant can conceivably contort the topology and set up courses under the control over the wormhole join.

• Sybilattack[18] incorporates a malicious device with the ability to illegitimately take on several identities in the same network. The forged identity from a malicious device is called a Sybil node. A malicious device can obtain an identity for a Sybil node in two different ways; (a) generating a new identity; or (b) taking the identity from an existing node (with the cooperation of the node or by developing a spoofing attack). We identify two types of Sybil attacks. In the first type, malicious nodes do not take part in finding routes, meaning that, legitimate nodes do not know their existence. In the second type, malicious nodes do create route advertisements and legitimate nodes are aware of the existence of malicious nodes, just do not know they are malicious. Some of the researchers have proposed many solutions for wormhole attack.

• Rushing assaults [19]. The ROUTE REQUESTs for this Disclosure sent by the aggressor are the first to achieve each neighbor of the objective, then any course found by this Route Disclosure will incorporate a jump through the assailant. That is, at the point when a neighbor of the objective gets the hurried REQUEST from the assailant, it advances that REQUEST, and won't forward any further REQUESTs from this Route Discovery. At the point when non-assaulting REQUESTs arrive later at these hubs, they will toss those honest to goodness REQUESTs.

• Blackmail [20]. The assault causes because of absence of credibility and it gifts procurement for any hub to degenerate other hub's true blue data. Hubs as a rule keep data of saw vindictive hubs in a boycott. This assault is significant against steering conventions that utilization system for the distinguishing proof of vindictive hubs and proliferate messages that attempt to boycott the guilty party. An assailant may manufacture such reporting messages and tell other hubs in the system to add that hub to their boycotts and segregate real hubs from the network [21].

3. SECURE ROUTING

The already introduced specially appointed directing conventions without security thought accept that every taking an interest hub do not vindictively disturbing the operation of the convention [22][23]. On the other hand, the presence of pernicious elements can't be dismissed in any framework, particularly in open ones like commercial hoc systems. Secure steering conventions adapt to vindictive hubs that can upset the right working of a steering convention by altering steering data, by creating false impersonating so as to direct data and different hubs. These protected steering conventions for impromptu systems are either totally new remain solitary conventions, or now and again fuses of security instruments into existing conventions. By and large the current secure directing conventions that have been proposed can be comprehensively ordered into two classifications, those that utilization hash chains, and those that keeping in mind the end goal to work require predefined trust connections. Along these lines, community oriented hubs can effectively validate the authentic movement and separate the unauthenticated bundles from outcast aggressors.

• SEAD [20]. Secure Efficient Ad hoc Distance vector directing convention (SEAD), a safe specially appointed system steering convention in light of the outline of the Destination-Sequenced Separation Vector directing protocol(DSDV) [24]. To bolster use of SEAD with hubs of restricted CPU preparing capacity, what's more, to make preparations for adjustment of the source address for a directing redesign and assaults in which a foreswearing of administration assaults endeavors to bring about different hubs to devour overabundance system transmission capacity or handling time, proficient restricted hash chains however not cryptographic operations are utilized as a part of the validation of the arrangement number and the metric (jump tally) field of a directing table upgrade message. At the point when a hub in SEAD sends a steering overhaul, the hub incorporates one hash esteem from the hash chain with every passage in that redesign. The hubs sets the destination address in that section to that destination hub's address, the metric and grouping number to the qualities for that destination in its directing table, and the hash worth to the hash of the hash esteem gotten in the directing overhaul passage from which it discovered that course to that destination. At the point when a hub gets a directing overhaul, for every passage in that redesign, the hub checks the confirmation on that passage, utilizing the destination location, grouping number, and metric in the got section, together with the most recent earlier legitimate hash worth got by this hub from that destination's hash chain. The hash estimation of every section is hashed the right number of times and it is contrasted with the already verified quality. Contingent upon this examination the steering redesign is either acknowledged as validated, or tossed.

• Ariadne [25]. Ariadne is a safe on-interest specially appointed steering convention taking into account DSR that avoids aggressors or bargained hubs from messing around with uncompromised courses comprising of uncompromised hubs, furthermore forestalls numerous sorts of Denial-of-Service assaults. Likewise, Ariadne uses just exceptionally productive symmetric cryptographic primitives. To persuade the objective of the authenticity of every field in a Course REQUEST, the initiator essentially incorporates into the emand a MAC (message confirmation code) processed with key over interesting information. The objective can without much of a stretch check the legitimacy and freshness of the ROUTE REQUEST utilizing the mutual key. Restricted hash capacities are utilized to check that no jump was excluded which is called per-bounce hashing. Three elective systems to accomplish hub list verification: the TESLA convention [26], computerized marks, and standard MACs. At the point when Ariadne Route Discovery is utilized with TESLA, each jump verifies the new data in the REQUEST. The target supports and does not send the REPLY until middle hubs can discharge the relating TESLA keys. Ariadne Course Discovery utilizing MACs is the most proficient of the three elective validation instruments, yet it requires pairwise shared keys between all hubs. The MAC list in the ROUTE Solicitation is processed utilizing a key shared between the objective what's more, the present hub. The MACs are checked at the objective and are not returned in the ROUTE REPLY. On the off chance that Ariadne Route Revelation is utilized with computerized marks, the MAC list in the Course REQUEST turns into a mark list.

• SRP [27].The Secure Routing Protocol (SRP) comprises of a few security expansions that can be connected to existing commercial hoc directing conventions giving end-to-end verification. The sole necessity of the proposed plan is the presence of a security relationship between the hub starting the question what's more, the looked for destination. The security affiliation is utilized to set up a mutual mystery between the two hubs, and the non-impermanent fields of the traded steering messages are ensured by this mutual secret. The plan is strong in the vicinity of various non-intriguing hubs, and gives precise steering data in an opportune way. No supposition in SRP is made with respect to the middle of the road hubs, which may display self-assertive and pernicious conduct. The SRP Header is incorporated into the basic convention header structure as an extra IP alternative, and covers most parts of the steering convention datagram. The source hub sends a course ask for with a question grouping (QSEQ) number that is utilized by the destination as a part of request to recognize obsolete solicitations, an arbitrary question identifier (QID) that is utilized to recognize the particular solicitation, and the yield of a keyed hash capacity. The destination hub figures the keyed hash of the solicitation fields. In the event that the yield coordinates the SRP header MAC, the honesty of this solicitation is checked, alongside the genuineness of its starting point. The destination produces various answers to legitimate solicitations, at most the same number of as the quantity of its neighbors, keeping in mind the end goal to deny a perhaps vindictive neighbor to control different answers. For each substantial solicitation, the destination hub places the aggregated course in the course answer parcel and the QID and QSEQ of the course ask for in the relating SRP header fields, so that the source hub can check the freshness of the answer. Hubs use secure message transmission (SMT) [28] to guarantee fruitful conveyance of information parcels. In SMT, information messages are split into bundles utilizing mystery sharing methods so that if M out of N such parcels are gotten, the message can be recreated. SRP ensures that created, bargained, or replayed course answers would either be rejected or never reach back the questioning hub.

• ARAN [29]. The Authenticated Routing for Ad hoc Systems (ARAN) taking into account AODV is a stand-alone convention that uses cryptographic open key declarations marked by a trusted power, which relates its IP address with an open key with a specific end goal to accomplish the security objectives of verification and non-denial. The convention accept that every hub knows from the earlier the general population key of the accreditation power that will be used to verify the other taking an interest hubs. ARAN utilizes cryptographic testaments to bring verification, message-honesty and non-revocation to the course revelation process. The source hub starts course instantiation to destination by television to its neighbors a course disclosure bundle (RDP). The RDP incorporates a bundle sort identifier, the IP location of the destination, the source hub's endorsement and a nonce, all marked with the source hub's private key. At the point when a hub gets a RDP message, it sets up an opposite way back to the source by recording the neighbor from which it got the RDP. The accepting hub utilizes the forerunner hub's open key and testament to accept the mark. The accepting hub signs the substance of the message, annexes its own testament, and forward shows the message to each of its neighbors. The mark keeps vindictive hubs from infusing discretionary course disclosure bundles that adjust courses or frame circles [30]. In the long run the RDP message is gotten, the destination unicasts a Reply (REP) parcel back along the converse way to the source. The REP incorporates a parcel sort identifier, the IP location of the source hub, the endorsement of the destination hub . Hubs that get the REP forward the parcel back to the forerunner from which they got the first RDP. Every hub along the opposite way back to the source signs the REP and adds its own particular endorsement before sending the REP to the following bounce. At the point when the source gets the REP, it confirms the destination's mark and the nonce returned by the destination. By utilizing cryptographic testaments that certifications end-to-end validation, ARAN limits or anticipates assaults that can harrow other frail conventions. ARAN is a straightforward convention that does not require noteworthy extra work from hubs inside of the gathering yet is as viable as AODV in finding and looking after courses. The expense of ARAN is bigger steering parcels, which bring about a higher general steering burden, and higher idleness in course disclosure on account of the cryptographic calculation that must happen.

• SAODV [31]. Securing AODV proposes an arrangement of augmentations that protected the AODV directing bundles. Two systems are utilized to secure the AODV messages: advanced marks to validate the non-changeable fields of the messages, and hash chains to secure the jump number data. Since the convention utilizes topsy-turvy cryptography for advanced marks it requires the presence of a key administration system that empowers a hub to get and confirm the open key of different hubs that take an interest in the impromptu system. At the point when a hub starts a course demand or a courseanswer message it sets the Max_Hop_Count field to the TimeToLive (TTL) field from the IP header, set a the hash field to arbitrary seed quality, computes Top_Hash by hashing arbitrary seed Max_Hop_Count times. A hub gets a course solicitation or a course answer message, it applies the hash capacity Max_Hop_Count short Hop_Count times to the quality in the Hash field, and checks that the resultant quality is equivalent to the quality contained in the Top_Hash field. In the event that the halfway hubs can answer to a course ask for the benefit of the last destination, the expansion of the mark is utilized to answer to the course mission. Generally the course demand will be sent by the moderate hubs.

• Securing connection state steering [32]. Secure Link-State Convention (SLSP) gives a proactive secure connection state steering answer for specially appointed systems. SLSP hubs scatter their connection state upgrades and keep up topological data for the subset of system hubs inside of R jumps, which is termed as their zone. Hubs' open key authentications are telecasted inside of their zone utilizing marked open key dissemination (PKD) bundles. Connection state data was shown intermittently utilizing Neighbor Location Protocol (NLP). While accepting a Connection state overhaul (LSU) parcels, hubs confirm the joined mark utilizing an open key they have beforehand stored in the pubic key conveyance period of the convention and confirm the jump tally by restricted hash chains. By securing the neighbor revelation process and utilizing NLP as a approach to recognize inconsistencies in the middle of IP and MAC addresses, SLSP offers insurance against individual vindictive hubs. In any case, SLSP is powerless against plotting assailants that create non-existing connections in the middle of themselves and surge this data to their neighboring hub.

4. MAODV ROUTE DISCOVERY AND SYBIL DETECTION PROCESS AND ANALYSIS

This paper proposed a modified sybil detection AODV protocol, which is based on the AODV protocol, could detect sybil attacks in the network in an efficient manner. In MAODV, a concept to detect Sybil attacks in the network by collecting both numbers of hop count and delay per hop information for different paths from source to destination, which offer a full general solution for both kinds of Sybil attacks. The reason behind is that under legitimate situation, the delay for each packet is similar along each hop in the path and the delay for each packet should be excessive for those nodes are involved in the Sybil attack because there can be many nodes between them or can be connected through a long link (wired or wireless). Therefore, if compare the delay per hop of every node in the normal path and a path that is under sybil attack, finds that delay per hop of a path that is under Sybil attack is larger in comparison of normal path. Therefore, if a path has a high delay per hop then this path can be under Sybil attack.

To avert the necessity of an extra hardware or monitoring system such as positioning system and a time synchronization mechanism such as directional antenna or intrusion detection system, MAODV protocol collects both delay and the number of hop count information in a similar way to the AODV route discovery process at the destination.

There are two steps process in our protocol to detect the sybil attacks in the network. In the first step, delay and number of hop count information is gathered at destination. In the second step, destination node starts the detection on the bases of the prior step knowledge.

Step 1: Receiver gathers information of each route from source to destination. Modified sybil detection AODV protocol uses two kinds of messages: MRreq and MRrep those are similar to the AODV Rreq and Rrep packets. MRreq is used by the sender node to find different routes to the destination, while MRrep message is sent from the destination node to the sender after a sybil detection process in the network, means destination node reply only for that route in which there are not possibility of sybil. MRreq packets let in a previous hop field, hop count field and a timestamp field and MRrep packet includes all fields like AODV reply packet protocol. When the sender starts route discovery process, it broadcasts an MRreq packet to the destination node, which is depicted in fig. 5.1. The MRreq packet includes the previous hop field, hop count field and the timestamp field. The previous hop field is occupied with sender's node ID, the hop count field is set to 1, and the timestamp field is filled with the time when the packet is sent. We use previous hop but not the whole route information because of saving the network resources. Many intermediate nodes process MRreq packet before reaching the destination node. Intermediate nodes can change only the previous hop field and hop count field but not timestamp field. Only the sender can modify Timestamp field.

When an intermediate node receives an MRreq packet, it reads the previous hop field and makes a reverse route to the sender and then replaces its node ID into the previous hop field and increases the hop count field by 1 and broadcast the modified MRreq packet to its neighbors.

Any node in the network broadcasts MRreq packets and set up a reverse route when it receives the packet first time. If any node receives, a request packet with same REQid then simply dropped it. In this protocol each request must reach to the destination, it does not matter that there is information to reach the destination in the routing table of the intermediate node.

When the destination node gets MRreq from its neighbor it does not immediately reply to the requested node. Instead of it collects information on each route from source to destination. Note that each MRreq packet carries the timestamp of the time when the sender sent the MRreq packet to the destination node and the hop count to reach the destination node (in AODV protocol, destination node replies to the first request received).

Step 2: in this step, after collecting information on each route from source to destination, destination node starts detection process. Suppose that the sender broadcasts the MRreq packet with source id, receiver id, source sequence number, destination sequence number and request id at time Ts and the destination node receives aMRreq packet from a neighbor node t at time Tt. The propagation time is given by PTt = Tt - Ts. Sequence numbers are used to remove the possibility of packet looping. If the hop count field in the MRreq packet from node t is Ht then the delay per hop value (DPHt) through node t to the destination node is given by

$$DPHt = \frac{PTt}{Ht} = \frac{Tt-Ts}{Ht} \qquad (1)$$

In the legitimate path, the delay per hop should be similar and routes those are affected with sybil attacks will have a larger delay per hop value than the legitimate route. Remember that two malicious nodes in the Sybil attack form an attacked and it does not matter how long tunnel is. An attacked can be formed directly from one malicious node to another malicious node or can be formed with the help of other nodes in the network.

We set T= 3ms, 4ms, 5ms, 6ms in the following simulations which measure the performance of MAODV. Fig 3 shows the simulation result for light background traffic when T=3ms, here light background traffic means we take only 100 requests. We commenced our simulation with the attacked length 2 hops because 1 hop is not considered as an attacked; here attacked length means hop count from M1 to M2. If the number of hop count from M1 to M2 is higher than the detection rate of the Sybil attack is also higher. The detection rate of the normal path is not dependent on the attacked length. When a path is under Sybil attack, then it does not matter that how long attacked path is; it always treated as 1 hop, hence H remains small. If the length of the attacked is small then the DPH of attacked path similar to that of a normal path, and the reason is that why a short-attacked path length leads to a lower detection rate.

Fig. 4 shows the result for medium background traffic when T=3ms. We took 250 requests in the medium background traffic. It is found that the detection rate of the attacked path is higher than that of light background traffic and detection rate of normal path is approximately same for each hop difference.

Fig. 5 shows the result for heavy background traffic when T=3ms. In heavy background traffic, we took 500 requests in the network. In the heavy background traffic, we found that the detection rate of attacked path increases for each hop counts and detection rate of normal path is also better than that of light background traffic and medium background traffic.

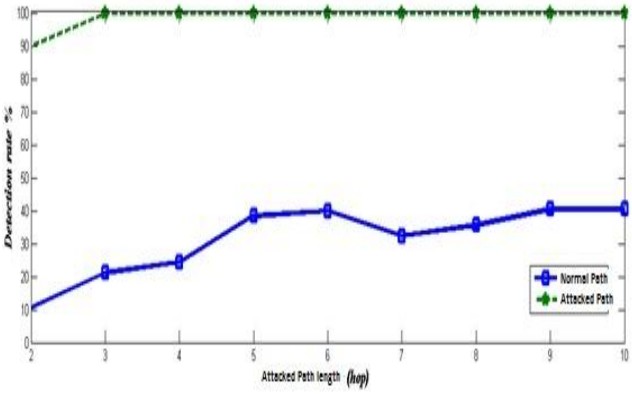

Fig 3: Light background traffic when T=3ms

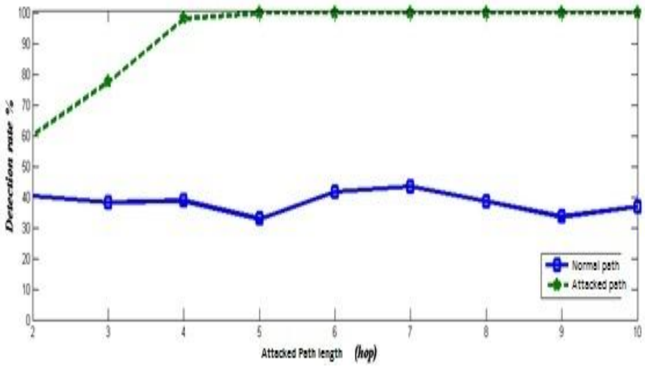

Fig 4: Medium background traffic when T=3ms

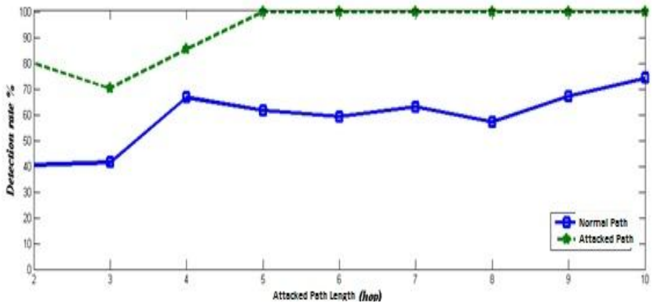

Fig 5: Heavy background traffic when T=3ms

Fig 6 shows the simulation result for light background traffic when T=4ms, here light background traffic means we take only 100 requests.

Fig. 7 shows the result for medium background traffic when T=4ms. We took 250 requests in the medium background traffic. It is found that the detection rate of the attacked path is higher than that of light background traffic and detection rate of normal path is approximately same for each hop difference.

Fig. 8 shows the result for heavy background traffic when T=4ms. In heavy background traffic, we took 500 requests in the network. In the heavy background traffic, we found that the detection rate of attacked path increases for each hop counts and detection rate of normal path is also better than that of light background traffic and medium background traffic.

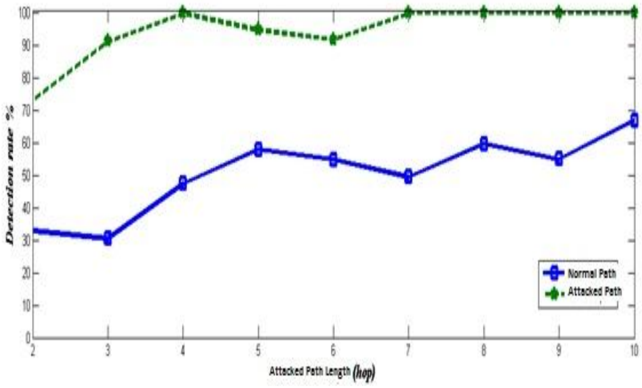

Fig 6: Light background traffic when T=4ms

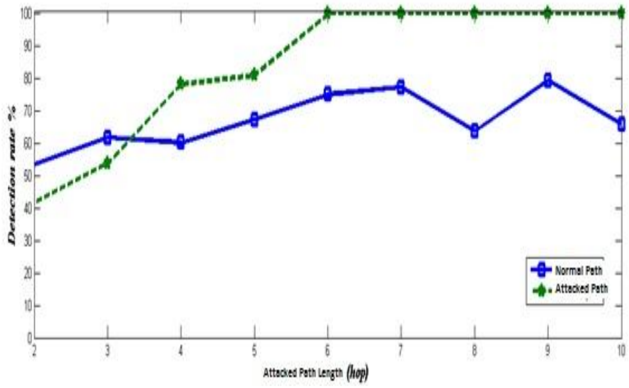

Fig 7: Medium Background Traffic when T=4ms

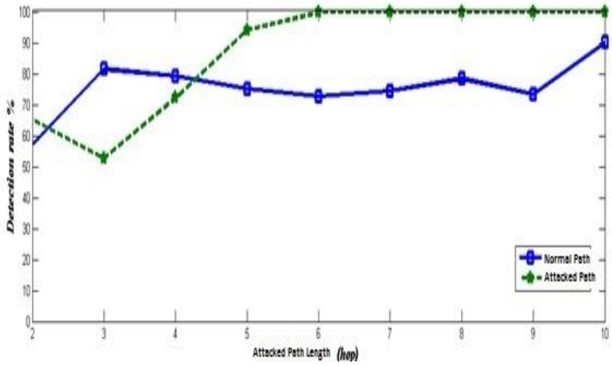

Fig 8: Heavy background traffic when T=4ms

Fig 9 shows the simulation result for light background traffic when T=5ms, here light background traffic means we take only 100 requests.

Fig. 10 shows the result for medium background traffic when T=5ms. We took 250 requests in the medium background traffic. It is found that the detection rate of the attacked path is higher than that of light background traffic and detection rate of normal path is approximately same for each hop difference.

Fig. 11 shows the result for heavy background traffic when T=5ms. In heavy background traffic, we took 500 requests in the network. In the heavy background traffic, we found that the detection rate of attacked path increases for each hop counts and detection rate of normal path is also better than that of light background traffic and medium background traffic.

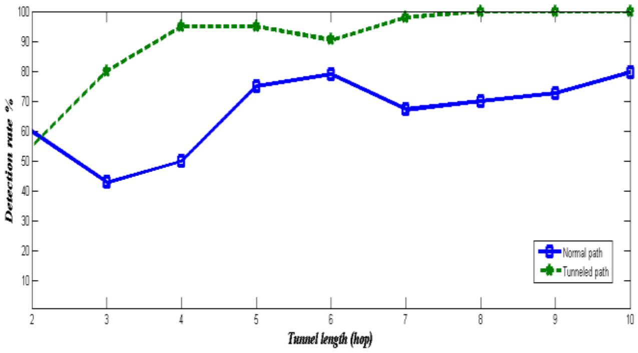

Fig 9: Light background traffic when T=5ms

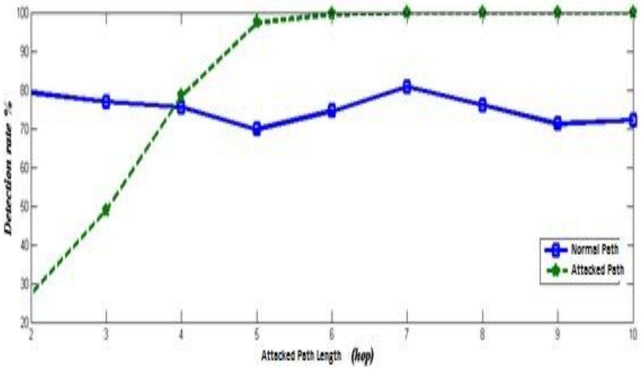

Fig 10: Medium background traffic when T=5ms

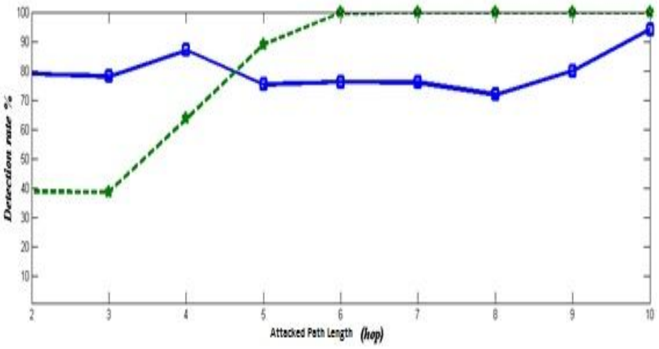

Fig 11: Heavy background traffic when T=5ms

Fig 12 shows the simulation result for light background traffic when T=6ms, here light background traffic means we take only 100 requests.

Fig. 13 shows the result for medium background traffic when T=6ms. We took 250 requests in the medium background traffic. It is found that the detection rate of the attacked path is higher than that of light background traffic and detection rate of normal path is approximately same for each hop difference.

Fig. 14 shows the result for heavy background traffic when T=6ms. In heavy background traffic, we took 500 requests in the network. In the heavy background traffic, we found that the detection rate of attacked path increases for each hop counts and detection rate of normal path is also better than that of light background traffic and medium background traffic.

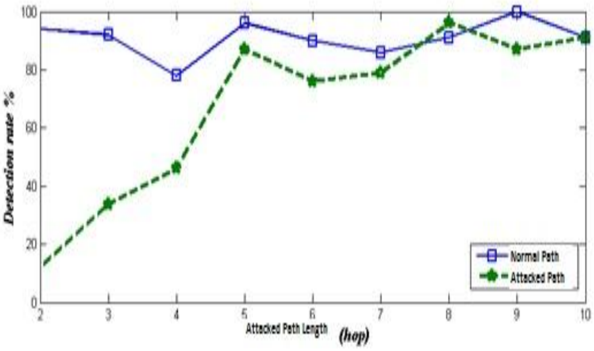

Fig 12: Low background traffic when T=6ms

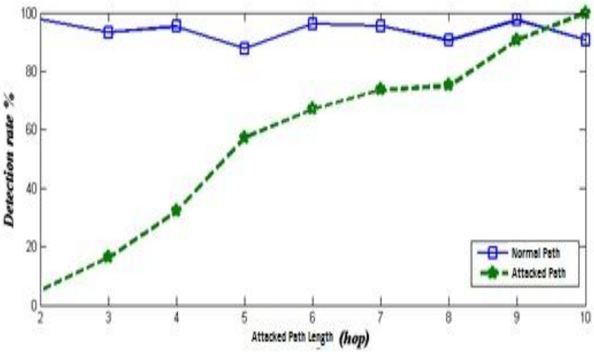

Fig 13: Medium background traffic when T=6ms

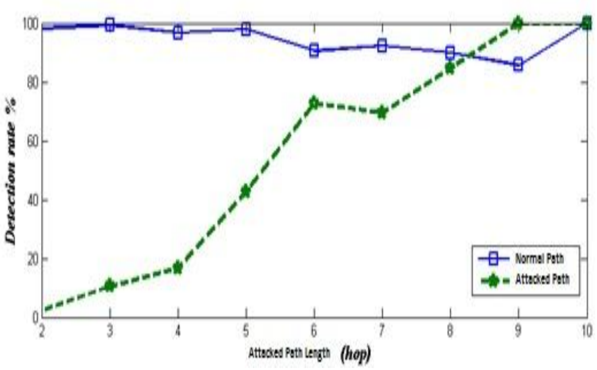

Fig 14: Heavy background traffic when T=6ms

5. CONCLUSIONS

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In this dissertation, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks with solution finding technique.

In this paper, we have focused on analyzing the Sybil attack, reviewing the previous approaches and proposing a new efficient solution. The MAODV protocol is able to detect both packet encapsulation and out-of-band channel Sybil attacks in the network. This solution does not require any cryptographic processing by the intermediate nodes in the absence of an attack, nor does it involve any packet overhead.

MAODV offers a verifiable solution to the Sybil attacks.

The main contributions of this paper are listed below.

A general introduction to the principal types of attacks that can be launched on ad hoc networks, in particular a detailed review and classification of Sybil attacks.

A complete survey of the most important approaches proposed to detect and prevent Sybil attacks in ad hoc networks.

An analysis of the Sybil attack and the accuracy of the existing solutions for preventing it.A new mechanism preventing sybil attacks in mobile ad-hoc networks called MAODV. Detection of sybil attack is performed using number of hops in different paths from source to destination and delay of each node in different paths from source to destination. The destination is able to detect both kinds of Sybil attacks.The advantages of modified Sybil detection AODV protocol are that it does not require any special hardware such as directional antenna and it does not require clock synchronization and positioning system.In this paper a new mechanism for detecting sybil attacks in ad hoc networks has been proposed. This mechanism can be improved in several ways. A list of possible future works related to this subject is presented and includes the following:

MAODV protocol does not work well when all the paths are sybil affected. So, how to enhance our modified sybil detection method to remove this situation andProviding reliability of MAODV is the future work.

6. REFERENCES

[1] Christian Lochert, Bj¨ornScheuermann, and Martin Mauve, A survey on congestion control for mobile ad hoc networks, Wireless Communications & Mobile Computing, Vol. 7, pp.655 – 676, June.2007

[2] TiranuchAnantvalee and Jie Wu, A Survey on Intrusion Detection in Mobile Ad Hoc Networks, Wireless Mobile Network Security, pp.170-196, 2003.

[3] Yongguang Zhang AndWenke Lee, Intrusion Detection in Wireless Ad-Hoc Networks, MOBICOM, 2000, pp. 275-283

[4] Andr´eWeimerskirch and Gilles Thonet, Distributed Light-Weight Authentication Model for Ad-hoc Networks, Lecture Notes In Computer Science; Vol. 2288, pp. 341 354, 2001

[5] I. Chlamtac, M. Conti, and J. Liu, Mobile Ad Hoc Networking: Imperatives and Challenges, Ad Hoc Networks, vol. 1, pp. 13-64, no. 1, 2003.

[6] L. Buttyan, J.P. Hubaux, Report on a working session on security in wireless ad hoc networks, Mobile Computing and Communications Review 6 (4), 2002.

[7] Ejaz Ahmed, KashanSamad, WaqarMahmood, Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks, AusCERT2006 R&D Stream Program, Information Technology Security Conference, May 2006, Australia.

[8] J.P. Hubaux, L. Buttyan, S. Capkun, The quest for security in mobile ad hoc networks, in: Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), October, 2001

[9] Shuyao Yu, Youkun Zhang, Chuck Song and Kai Chen, A security architecture for Mobile Ad Hoc Networks, Available:http://blrc.edu.cn/blrcweb/publication/kc2.pdf .

[10] J. Lundberg, Routing Security in Ad Hoc Networks, 2000.Availabe: http://citeseer.nj.nec.com/400961.html.

[11] HAO YANG, HAIYUN LUO, FAN YE, SONGWU LU andAND LIXIA ZHANG, Security in mobile ad hoc networks: Challenges and solutions, IEEE Wireless Communications, vol. 11, pp. 38-47, Feb., 2004.

[12] IoannaStamouli, “Real-time Intrusion Detection for Ad hoc Networks”, M. Sci. dissertation, University of Dublin, 2003

[13] F. Stajano, and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks,” Proc. 7th Int’l. Workshop on Security Protocols, Cambridge, UK, April 1999, pp. 172-194.

[14] J.-F. Raymond, “Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems,” Proc. Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, July 2000, pp. 7-26.

[15] Bo Sun, Kui Wu, Udo W. Pooch. Alert aggregation in mobile ad hoc networks.Proc. ACM workshop on Wireless security, 2003.

[16] M. Drozda, H. Szczerbicka. Artificial Immune Systems: Survey and Applications in Ad Hoc Wireless Networks.Proc. 2006 International Symposium on Performance Evaluation of Computer and

Telecommunication Systems (SPECTS'06), pp. 485-492, Calgary, Canada, 2006.

[17] P. Papadimitratos, and Z.J. Haas, “Securing the Internet Routing Infrastructure,” IEEE Communications, vol. 10, no.40, October 2002, pp. 60-68.

[18] Y.-C. Hu, A. Perrig, and D.B. Johnson, “Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Networks,” Proc. 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom’03), San Francisco, CA, April 2003

[19] Yih-Chun Hu, Adrian Perrig, and Dave Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols."In Proceedings of the ACM Workshop on Wireless Security (WiSe), San Diego, California, September 2003.

[20] Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks,” Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.

[21] L. Zhou, and Z.J. Haas, “Securing Ad hoc Networks,” IEEE Network Magazine, vol. 6, no. 13, November/December 1999, pp. 24-30.

[22] D.B. Johnson, D.A. Maltz, Y.-C.Hu, and J.G. Jetcheva, The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR), Internet Draft, draft-ietf-manet-dsr-07.txt, February 2002.

[23] C.E Perkins, E.M. Royer, and S. Das, “Ad hoc On-demand Distance Vector (AODV),” RFC 3561, July. 2003.

[24] C.E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Proc. SIGCOMM ’94 Conf. Communications Architectures, Protocols and Applications, ACM Press, 1994, pp. 234–244.

[25] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks."In Wireless Networks Journal, 11(1), 2005.

[26] A. Perrig, R. Canetti, D. Song and J.D. Tygar, Efficient and secure source authentication for multicast, in: Proceedings of the Network and Distributed System Security Symposium, NDSS’01 (February 2001) pp. 35–46.

[27] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation (CNDS), January 2002.

[28] P. Papadimitratos and Z.J. Haas, “Secure Message Transmission in Mobile Ad Hoc Networks,” Elsevier Ad Hoc Networks J., Elsevier, vol. 1, no. 1, 2003, pp. 193–209.

[29] KimayaSanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding-Royer, “Authenticated Routing for Ad Hoc Networks”, Proceedings of IEEE journal on selected areas in communications, Volume 23, No. 3, March 2005

[30] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, “A Secure Routing Protocol for Ad hoc Networks”, Proc. 10th IEEE Int’l. Conf. Network Protocols (ICNP’02), IEEE Press, 2002, pp. 78-87.

[31] M.G. Zapata, N. Asokan, Securing ad hoc routing protocols, in: Proceedings of ACM Workshop on Wireless Security (WiSe), Atlanta, September 2002.

[32] P. Papadimitratos, and Z.J. Haas, “Secure Link State Routing for Mobile Ad hoc Networks,” Proc. IEEE Workshop on Security and Assurance in Ad hoc Networks, IEEE Press, 2003, pp. 27-31.