International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-2 Issue-15 June-2014

Defence Mechanism for SYBIL Attacks in MANETS using ABR Protocol

Sowmya P[1], V. Anitha[2]

Abstract

Security is of paramount concern in any adhoc network. In Mobile Adhoc NETworks (MANETs), mobility of the nodes poses a problem for providing security services [1]. The ad-hoc network is more vulnerable to attacks, since it uses wireless communication link between the mobile nodes. Sybil Attack is a spoofing attack, where a malicious node illegitimately creates multiple fake identities (called the Sybil nodes) to impersonate as normal nodes. It is observed that most of the existing protocols fail to defend against Sybil attack. Associativity Based Routing (ABR) protocol is an on-demand active routing protocol. It chooses the most long lived and stable route for communication rather than the shortest route. In this paper, using ABR protocol, we show that a legitimate node in the network along with the Local Server (LS) can detect the Sybil attacker. We show through simulation that using the concept of a PKI secured SESSION KEY (SESS_KEY), we can detect the presence of a Sybil attacker in the network. The empirical results show that there is an increase of 10% in the throughput and 60% in good put and the integrity of the network. This would lead to a more secure communication network with a reduced overall delay.

Keywords

Sybil, Associativity, ABR, MANETS.

1. Introduction

MANETs is promising new technology which has made a major landmark in the field of wireless communication to enable economically viable solutions.

This work was supported in part by the Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bangalore, India.

Manuscript received April 27, 2014.

Sowmya P, M. Tech - Final Year, Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bangalore, India.

V. Anitha, Associate Professor, Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bangalore, India.

With the mobile nodes constituting the network, the network does not have any fixed infrastructure and uses a wireless communication link between the nodes for communication. These networks provide viable solutions for many applications like traffic monitoring, pollution sensing, etc. The probability of network malfunctioning and uncontrolled behaviour is very high in MANETs, as they are deployed in very harsh or abnormal conditions [2]. These network applications require security, especially if the network protects or monitors critical infrastructures. A few attacks to which MANETs are highly vulnerable are Sybil Attack [3], Gray Hole Attack, Worm Hole Attack, Flooding Attack, on-off attacks, DDOS attacks [4-7], spoofing attacks. Impersonation attacks [8] or the spoofing attacks like the Sybil attack is the one where a malicious node claims to have multiple identities. These multiple identities are the Sybil nodes. This attack is a serious threat to the network as it hampers the important functions of a network like routing, resource allocation, message integrity, etc. In the network, each node represents a unique address. In Sybil attack, the attacker represents its multiple identities with several addresses. The malicious node identifies itself as another legitimate node in the network and thus any message directed to the victimized node is received by the malicious node. The ABR protocol [9] is a reactive on-demand routing protocol which gives a stable and long lived route from the source to the destination. It chooses the route based on the property of "Associativity" and discards all the other routes. This paper mainly deals with the defense mechanism proposed using the Direct Validation technique [3], where a node directly validates another node with the help of a secure and unique PKI based SESSION KEY (SESS_KEY), generated by a central authority called the Local Server (LS) which confirms the identity of one node with the other nodes in the network.

Thus SESS_KEY allows the node to establish a secure link to other nodes. This paper analyses and makes a comparison of the various defense mechanisms applicable for the different types of attack models. This paper aims at implementing a PKI based ABR protocol to provide a stable, long lived and secure route. Using the PKI based ABR

protocol; the throughput of the system can be improved. The paper is organized as follows: In section 2, the literature review is discussed. ABR protocol is discussed in section 3. Section 4 deals with the concept of Sybil Attacks. Public Key Infrastructure (PKI) is discussed in section 5. The problem statement of the paper and the proposed work along with the state machine diagrams and the flowcharts of the proposed defense mechanism are discussed in detail in section 6. Section 7 shows the simulation results. The conclusion and future work is discussed in section 8.

2. Literature Review

The Sybil attack was first described by Douceur in the context of peer-to-peer networks [10]. It was noted by Karlof and Wagner that the Sybil attack poses a threat to routing mechanisms in sensor networks [11]. Newsome, *et al.* [3] proposed several methods for detecting Sybil entities in a sensor network. They introduced taxonomy of the different forms of the Sybil attack and its defenses in wireless sensor networks. C. Piro, *et al.* [12] proposed that mobility of the nodes in a wireless network can be used to detect the presence of Sybil nodes in the network. They proposed two passive methods which show how individual mobile nodes can detect a Sybil attacker. Sarit Pal, *et al.* [13] also proposed different techniques to defend against Sybil attack in MANETs. ABR is an on-demand routing protocol that can be used in routing for MANETs to provide long lived stable route using the concept of "Associativity". C.-K. Toh, *et al.* [9] [14] [15] have proposed and explained the working of the ABR Protocol with a new metric called the "Associativity" between the neighbouring nodes which stabilizes the route and prevents frequent breakage in links. Anitha V., *et al.* [16] introduced the concept of overhearing and threshold in Enhanced ABR (EABR) protocol to fight against malicious nodes.

Ray Hunt [17] discusses the several issues associated with the use of PKI and in managing the processes, keys and certificates. He also throws light on the *Time stamping* service and the data certification which supports the *non-repudiation* property of PKI. Fongen [18] discusses a range of technologies for securing and separating different networks including the recent technology such as the Android Technology.

3. ABR Protocol

ABR protocol is a bandwidth efficiently distributed protocol [9] used in Ad-hoc networks. It is an On-Demand routing protocol initiated by the source (SRC). The destination (DEST) node decides on the route to be chosen based on the property of "Associativity" and discards all the other routes. Hence this is called as a "Long-lived" routing protocol.

Property of Associativity:
The property of Associativity [9] states that a node's association with its neighbour changes as it migrates and its transiting period can be identified by the associativity "ticks". After the unstable period of migration, the node will spend some stable dormant time within a wireless cell before it transits again. The threshold where the associativity transitions take place is defined by $A_{threshold}$. The node periodically transmits beacons identifying itself and constantly updates its associativity ticks with the nodes in its vicinity. Any associativity ticks greater than this threshold implies periods of association stability.

Phases of ABR:
The 3 main phases in the ABR protocol are:

a. Route Discovery phase
b. Route Reconstruction phase
c. Route Deletion phase

Route Discovery Phase:
Route Discovery Phase is the first phase involved in the ABR protocol. It uses two queries – Broadcast query (BQ) and BQ- Reply. The source node desiring a route will broadcast a BQ message searching for nodes having route to the destination. All the nodes receiving this message will append their addresses and their associativity ticks with the neighbours. Every successor node will erase its upstream node neighbour's associativity tick entries and retains only the entry concerned with itself and its upstream node. In this way, each packet arriving at the destination will contain the associativity ticks of the nodes which are in the route to the DEST. DEST will select the best route by examining the associativity ticks along each path. In case there are multiple paths having the same degree of association stability, then the route with the minimum number of hops will be selected. The DEST now sends a REPLY packet back to the SRC along this path. The nodes which propagate the REPLY will mark their routes as valid. All the other routes will remain inactive and this avoids the

possibility of duplicate packets arriving at the destination.

Route Reconstruction Phase:
The Route Reconstruction Phase is triggered when either of the nodes such as SRC, DEST or intermediate nodes moves. The following operations may be invoked when the nodes move for route maintenance:

a. Partial route discovery
b. Invalid route erasure
c. Valid route update
d. New route discovery (worst case)

Route Deletion Phase:
When a discovered route is no longer desired, SRC initiates Route Delete (RD) message to delete the route. The SRC broadcasts this message since it is not be aware of any route node changes that might have occurred during the route re-constructions. All the intermediate nodes update their routing table entries.

4. Sybil Attack

Sybil Attack is a serious threat in Ad-hoc networks as it impacts the functions of the network. In this attack, the malicious node claims to have multiple identities. These multiple identities are the Sybil nodes. The malicious node identifies itself as another legitimate node in the network and thus any message directed to the victimized node is received by the malicious node. This attack, thus detriment the important functions of a network like routing, resource allocation, message integrity, etc. In the network, each node represents a unique address. In Sybil attack, the attacker represents its multiple identities with several addresses. Thus these Sybil nodes in several different routes can gather information pieces from each of the route and puts them all together to make relevant information and thus alter the packets towards the same destination [13].

The three taxonomies for Sybil Attack are [3]:
Direct and Indirect Communication: In Direct communication, the Sybil nodes and the legitimate nodes interact with each other directly. When a legitimate node sends a message to a Sybil node, the malicious node listens to this message. Similarly, the messages sent from Sybil nodes are actually the messages sent from the malicious node. In Indirect communication, the legitimate nodes cannot directly interact with the Sybil nodes. Instead, they communicate with one or more of the malicious nodes which claim to reach the Sybil nodes.

Fabricated and Stolen Identities: A Sybil node can get its identity in two ways. It can either fabricate a new identity (similar to that of a legitimate node) or can steal an identity from one of the legitimate nodes.

Simultaneity: In Simultaneous attack, the attacker tries to have all the Sybil nodes participate in the network at once. In Non-simultaneous, the attacker tries to have only a part of his Sybil identities to participate in the network at any given point of time. The attacker does this by making to seem that one identity is leaving the network and another identity is joining its place.

A few forms of Sybil Attack are [3]:

Distributed Storage: Sybil Attack could easily defeat repetition and fragmentation mechanisms. Suppose the system is designed to replicate or fragment the data across several nodes, with Sybil attack it could actually be storing the data on the different identities of the Sybil attacker.

Routing: Sybil attack could defeat routing algorithms as well. It could defeat the concept of having disjoint paths to the same destination, by having the various routes pass through a single malicious node. The Sybil identities could be spread across these various paths.

Data Aggregation: A few network protocols use the aggregated values rather than the individual values in the network to conserve energy. The presence of the Sybil attacker could hamper the aggregate reading.

Voting: Networks could use voting for various tasks. Sybil attack could use two types of attacks like “stuff the ballot box” or “blackmail” attacks. In “stuff the ballot box” attack, the malicious node casts the vote in its favour using its Sybil identities. The malicious attacker can determine the outcome of any vote, since he knows the number of identities he owns. He could use this to “blackmail” a legitimate node that it is misbehaving.

Fair Resource Allocation: Some networks allocate resources on a per node basis. Using Sybil attack, a malicious node can obtain an unfair share of the resources. This reduces the resource access to the

legitimate node and gives the attacker more resources to perform more attacks.

Misbehaviour Detection: Suppose the network can detect a specific type of misbehaviour, it will wait for several repeated offenses by the same node before it takes any action. The Sybil attacker could "spread the blame" by taking care that not one Sybil identity misbehaves for the system to take action. Even if one of the Sybil identities is offended and revoked, then the attacker can continue misbehaving using new Sybil identities, never getting revoked himself.

5. Public Key Infrastructure (PKI)

PKI [17] plays an important role in providing security services such as authentication, confidentiality, integrity and digital signatures. It has the property that given an encryption key, it is infeasible to compute the decryption key and vice versa [18]. PKI has increased security and convenience when compared to other encryption methods. It also has the property of *non-repudiation* where the user has the sole responsibility for protecting his or her private key. Users who are widely spread over a large area can securely communicate through a chain of trust using PKI. The components of PKI are:

a. Security Policy
b. Certification Authority (CA)
c. Registration Authority (RA)
d. Certificate Repository and distribution system
e. PKI-enabled applications

6. Proposed Work

In our proposed work, we are detecting the presence of malicious Sybil node in the very first phase of ABR i.e. the Route Discovery Phase. We use the concept of Direct Validation where a node directly tests whether another node is valid or not. We try to detect the malicious node while it is trying to initiate communication with a legitimate node in the network. A PKI secured unique SESS_KEY allows the node to establish a secure link to other nodes. A new node in the network has to register itself with the servers such as the Local Server (LS) and the Central Server (CS). LS are the server in the area where the node would participate in the network. CS is the central authority which manages all the nodes in the network. These servers are the identification authorities which confirm the identity of one node with the other nodes in the network. As a first step, the node has to register itself with LS, for which it has to share its unique identification (UID) with LS. The UID for the node is generated using the concept of simplified version of the Data Encryption Standard (DES) [19] as shown below in (1). UID = fn (MAC address of the node)(1) Fig. 1 explains the function on the MAC address using the simplified version of DES to generate the UID.

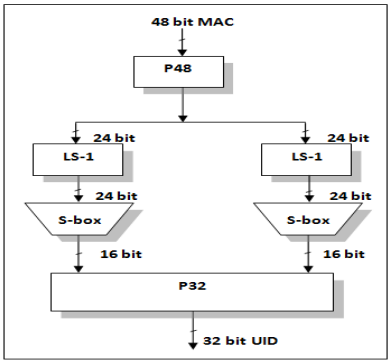

Fig. 1 UID generation using simplified DES.

The 48- bit MAC address of the node is divided into two sequences each of 24 bit. Each sequence is left shifted by 1 bit. Each 24 bit sequence is reduced to 16 bit sequence using the DES S-box. The two 16 bit sequences are concatenated to give the 32 bit UID of the node. The LS generates a secure unique session key SESS_KEY for this UID as shown in (2)
SESS_KEY = fn (UID + Timestamp)(2)
LS shares the generated SESS_KEY with the node and the Central Server (CS). CS then registers the node in the network. This completes the registration of the node in the network. Fig. 2 shows the state diagram for a new node registration in the network. Fig. 3 shows the State Diagram for the action taken by the LS during the registration of a new node.

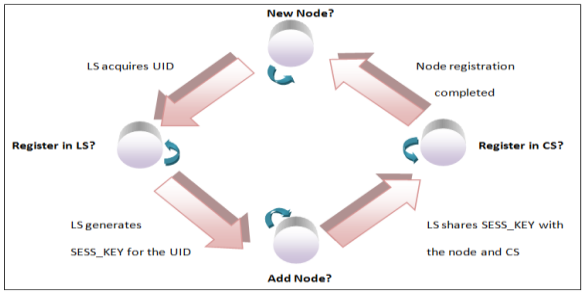

Fig. 2 State Machine Diagram for the registration of a new node.

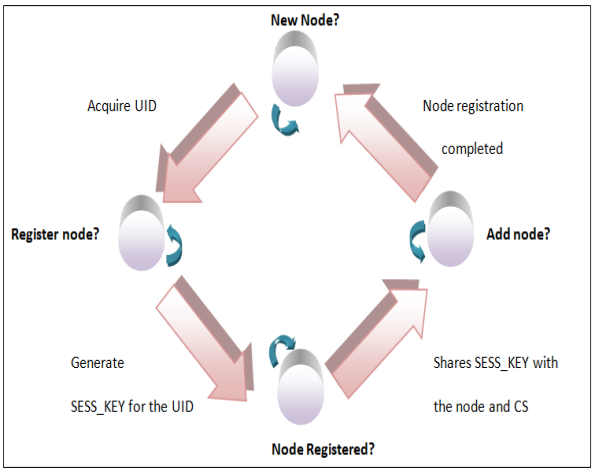

Fig. 3 State Machine Diagram for the registration of a new node – Action taken by LS.

Once the node is registered, it is eligible to communicate with the other nodes in the network. Sybil attacker tries to hamper the network communication during message transfer. The attacker or its Sybil nodes could acquire identification similar to that of the legitimate nodes and try to participate in the network. During the route discovery phase, when there is a search for a long lived route using ABR protocol and LQ packets being exchanged between the nodes, the Sybil node might attempt to identify itself as a legitimate node and might pose to have a route to the destination. Our proposed work attempts to identify the Sybil node and prevent the participation of the malicious node in the route.

Any node A which wants to communicate with another node B in the network has to share its UID and the PKI secured unique SESS_KEY with node B. Node B sends the UID and SESS_KEY for verification to LS to which node A belongs. LS now compares the UID and the SESS_KEY with those of the registered node. After comparing, LS sets the bit SECURE_ID as 1 or 0, '1' if it is a legitimate node and '0' if it is a Sybil node. If SECURE_ID = 1, then it indicates that node A is a legitimate node and LS now intimates Node B that it can commence communication with node A as shown in Fig. 4. Suppose node A is a Sybil node, then there is a mismatch between the secure unique SESS_KEY generated by the LS and the SESS_KEY provided by node A (Sybil node). LS now sets the bit SECURE_ID = 0 and alerts Node B, CS and all other local nodes about the presence of the Sybil node.

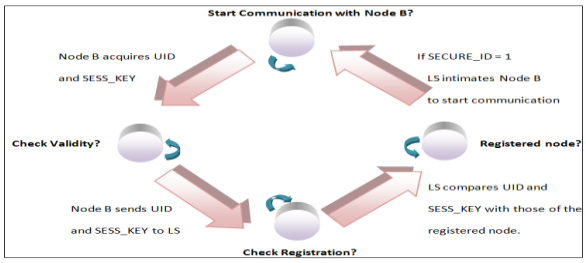

Fig. 4 State Machine Diagram for Message Transfer.

CS broadcasts a message to alert all the nodes in the network about the Sybil node and deletes this node from the network. Fig. 5 shows the state diagram for the action taken by LS during message transfer.

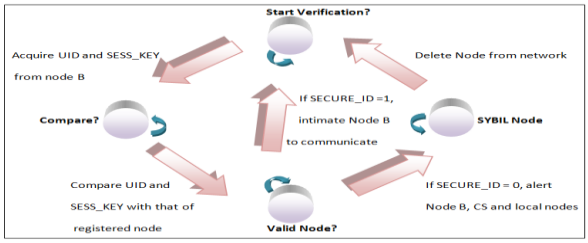

Fig. 5 State Machine Diagram for Message Transfer – Action taken by LS.

Fig. 6 shows the flow control for the registration of a new node in the network. Fig. 7 shows the flow control for the detection of a Sybil node when it is trying to communicate with a legitimate node in the network.

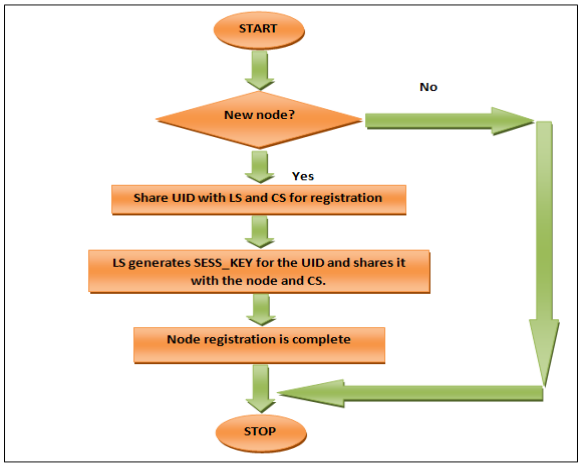

Fig. 6 Flowchart for the registration of a new node in the network.

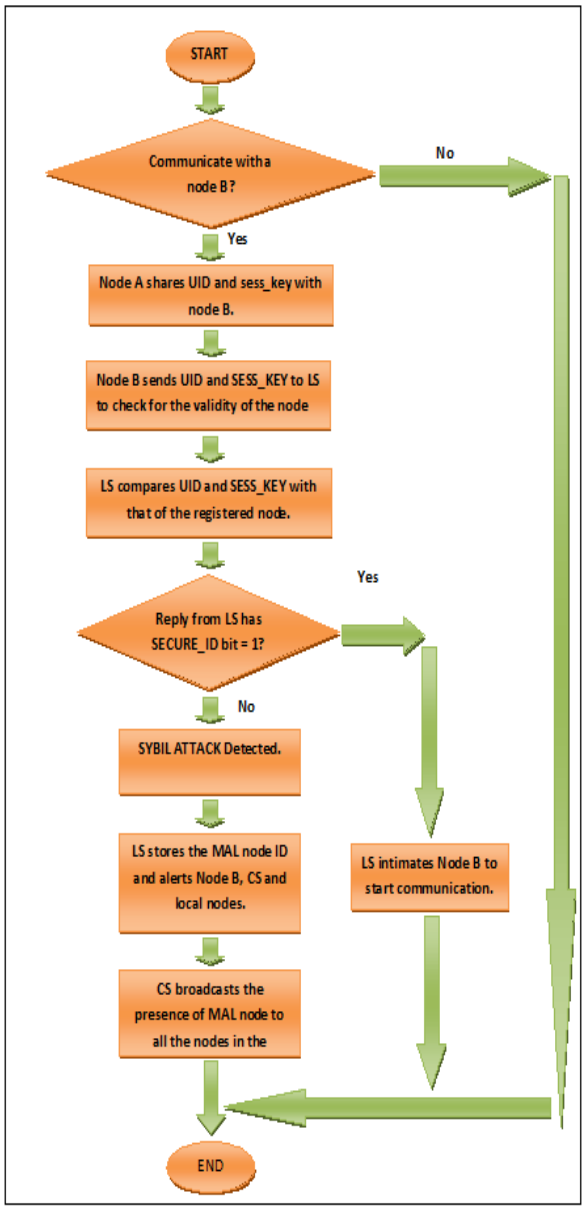

Fig. 7 Flowchart for the detection of a Sybil node when it is trying to communicate with another legitimate node in the network.

7. Simulation Results

The following are the simulation results obtained:
The simulation studies involve the deterministic network topology with 50 nodes. The proposed algorithm is implemented with NS2. The simulation parameters were set as illustrated in Table 1.

Table 1 NS2 simulation settings

Simulation Parameter	Value
Network Scale	800m x 800m
Simulation time	900s
Number of nodes	50
Mobility model	Random way point
Maximum nodes velocity	5m/s
Traffic Type	CBR
Connections number	10,20,30
Packets Transmission Rate	4 Packets/sec
Initial Energy	10J
Transmission Power	0.4W
Reception Power	0.2W

The proposed algorithm is compared between two protocols, the ABR protocol and our Sybil Free ABR (SFABR) protocol. Our results show that SFABR performs better than ABR in terms of throughput, end to end delay and good put. The malicious node is detected in the route discovery phase of ABR when the LS sets the bit SECURE_ID = 1.

Throughput:

In communication networks, *throughput* of the system is defined as

Throughput = Number of packets received / Total number of packets delivered.

It is measured in terms of *bits per second* (*bps*) or data packets per second. It is observed that the system with SFABR has an improved throughput of around 10% than the system with ABR protocol as shown in Fig. 8. Thus, we can conclude that SFABR efficiently utilizes the bandwidth than ABR protocol.

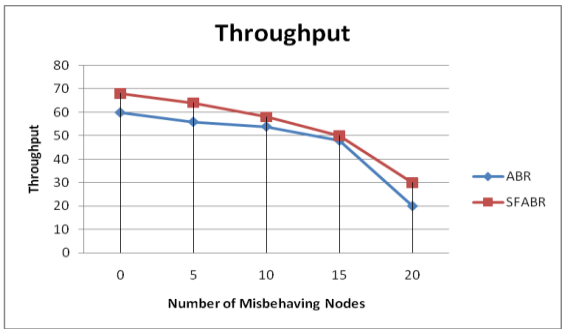

Fig. 8 Throughput.

End to End Delay:

Next, we compare the end to end delay using both ABR and SFABR protocols in the systems. In communication networks, *end to end delay* is defined as the time taken by a packet to be transmitted across

a network from the source to the destination. It involves the transmission delay, the propagation delay, the processing delay and the queueing delay. It is measured in *seconds*. It is observed that SFABR has reduced end to end delay by 5% when compared to ABR as shown in Fig. 9. Thus, we can conclude that SFABR improves the efficiency of the system.

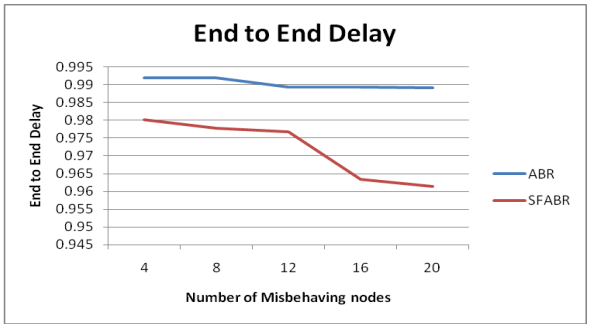

Fig. 9 End to end delay.

Good Put:

Good put gives the actual data rate of any communication network. *Good put* is defined as

Good Put = Number of packets received successfully / Total number of packets delivered.

It is related to the amount of time from the first bit of the first packet delivered until the last bit of the last packet is delivered. In our results, we have observed that the good put as observed is better by 60% in SFABR than ABR protocol and this is shown in Fig. 10.

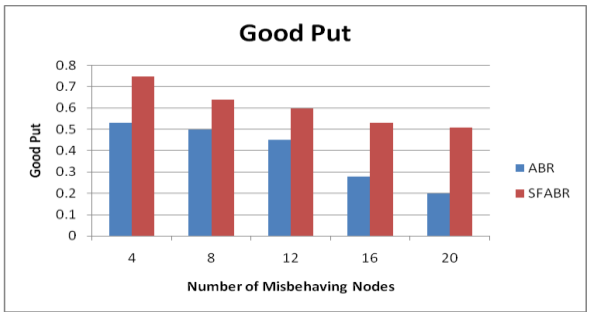

Fig. 10 Good Put.

The results thus show that the improvement achieved by detecting and removing the malicious nodes in the network during the route discovery phase of ABR contributes to the performance improvement.

8. Conclusion and Future Work

Establishing a secure, tamper-resistant, stable and long lived route, free from malicious nodes is a challenging task. Sybil Attack is a harmful attack in MANETs, where a malicious node behaves as if it were a larger number of nodes either by impersonating other nodes or by claiming false identities. Here in this paper, we propose to detect the presence of the attacker in the Route Discovery Phase of ABR using PKI secured unique SESSION KEY (SESS_KEY) generated by the Local Server (LS) during the time of the registration of a node into the network. This would thus lead to a secure communication network with a reduced overall delay and yields an efficient increase in the throughput, good put and integrity of the network. In our future work, we propose to work on detecting the presence of the Sybil attacker in the other phases of ABR.

References

[1] L. Zhou, and Z. J. Haas, "Securing Ad Hoc networks," IEEE Network, Vol. 13 No. 6, pp. 24-30, 1999.

[2] Dr. Sunilkumar S.Manvi, Mahabaleshwar S.Kakkasageri, "Wireless and Mobile Networks: Concepts and Protocols", Wiley India Pvt. Ltd., 2010.

[3] J. Newsome, E. Shi, D. Song and A. Perrig. "The Sybil Attack in Sensor Network: Analysis & Defenses." IPSN'04, April 26–27, 2004, Berkeley, California, USA.

[4] Ms. Neetu Singh Chouhan, Ms. Shweta Yadav, "Flooding Attacks Prevention in MANET", International Journal of Computer Technology and Electronics Engineering (IJCTEE), ISSN 2249-6343, Volume 1, Issue 3, 2011.

[5] N. Balaji, A. Shanmugam "Dynamic Trust Based method to Mitigate Greyhole Attack in Mobile Adhoc Networks", International Conference on Communication Technology and System Design 2011.

[6] Megha Arya, Yogendra Kumar Jain "Greyhole Attack and prevention in Mobile Adhoc Network" International Journal of Computer Applications (0975-8887) volume 25- No.10, August 2011.

[7] Neeraj Sharma, B.L. Raina, Prabha Rani, Yogesh Chaba, Yudhvir Singh, "Attack prevention methods for DDOS attacks in MANETs"-Asian Journal Of Computer Science And Information Technology1:1 (2011) 18 – 21.

[8] D. Glynos, P. Kotzanikolaou, and C. Douligeris, "Preventing impersonation attacks in MANET with multi-factor authentication," Proceedings of

the Third International Symposium on Modelling and Optimization in Mobile, Ad Hoc and Wireless Networks, pp. 59-64, 2005.

[9] C.K Toh, "Associativity Based Routing for Ad-Hoc Mobile Networks", Wireless Personal Communications 4: 103–139, 1997.

[10] J. R. Douceur, "The Sybil Attack", Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS), March 2002.

[11] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113-127, May 2003.

[12] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile Ad Hoc networks," Proceeding of the Second International Conference on Security & Privacy in Communication Networks, Edited by Mukesh Singhal & John Baras Baltimore, M.D.: IEEE press, 2006.

[13] Sarit Pal, Asish K. Mukhopadhyay, and Partha Pratim Bhattacharya, "Defending Mechanisms Against Sybil Attack in Next Generation Mobile Ad Hoc Networks" - IETE TECHNICAL REVIEW, Vol. 25, ISSUE 4, JUL-AUG 2008.

[14] Elizabeth M. Royer, C.K.Toh., "A Review of current Routing Protocols for AD Hoc Mobile Wireless Networks". IEEE Personal Communications, (1070-9916/99)1999.

[15] C.K.Toh, "AD-Hoc Mobile Wireless Networks: Protocols and Systems", Englewood, Cliffs: Prentice Hall, 2002.

[16] Anitha Vijaya Kumar, Akilandeswari Jeyapal, Rohith Gowda, "FPGA Implementation of Enhanced ABR Protocol with Auto Defense towards Malicious Node in MANETs", Internal Security, ISSN 2080-5268, July-December 2012: 137-154.

[17] Ray Hunt, "PKI and Digital Certification Infrastructure", Proceedings of the 9th IEEE International Conference on Networks (ICON'01), 2002.

[18] Fongen, A., "Optimization of a Public Key Infrastructure", 2011 Military Communications Conference.

[19] William Stallings: Cryptography and Network Security, Principles and Practice, PHI.

Sowmya P received her Bachelor of Engineering in Electronics and Communication in 2004 from Visvesvaraya Technological University (VTU), Belgaum, Karnataka. She has worked as Senior Software Engineer in Infosys Technologies Limited, India for 6 years. She is currently pursuing her Final Year M.Tech in the Department of Electronics and Communication from VTU in Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.

Anitha V received her Bachelor of Engineering in Electronics and Communication from Bharathiyar University in 2000 and her Master of Engineering in Applied Electronics from Anna University, Chennai, in 2004. She has a teaching experience of more than 10 years. She has published more than 13 research papers in National/International journal Conferences. Currently she is working as an Associate Professor in the Department of Electronics and Communication Engineering in Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.