ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

EFFECTIVE ALGORITHM FOR REDUCED PACKET LOSS IN SYBIL ATTACKS

Dr. C. N. Shighe

Professor

Beijing University of Technology

Beijing, China

ABSTRACT

Wireless as well as mobile ad hoc networks are vulnerable to different attacks from multiple sources. These attacks are classified in the taxonomy of active and passive attacks. Sybil attack is one of the majorly used and implemented attacks in the network community to sniff the identity and use the same for further usage. Recently, there has been much excitement in the research community over using social networks to mitigate multiple identity or Sybil Attacks. A number of schemes have been proposed, but they differ greatly in the algorithms they use and in the networks upon which they are evaluated. As a result, the research community lacks a clear understanding of how these schemes compare against each other, how well they would work on real-world social networks with different structural properties, or whether there exist other (potentially efficient) ways of Sybil defense. In the event of a Sybil strike, the gatecrasher subverts the notoriety arrangement of system framework by making a substantial number of pseudonymous characters, utilizing them to addition a lopsidedly huge impact. A notoriety framework's weakness to a Sybil strike relies on upon how efficiently personalities could be created, the degree to which the notoriety framework acknowledges inputs from substances that don't have a chain of trust connecting them to a trusted substance, and whether the notoriety framework treats all elements indistinguishably. Confirmation demonstrates huge scale Sybil ambush might be completed in an exceptionally shoddy and effective path in the reasonable framework like Bittorrent Mainline. A

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

substance on a distributed system is a bit of programming which has entry to neighborhood assets. An element publicizes itself on the distributed system by exhibiting a character. More than one character can relate to a solitary substance. In this research paper, an effective methodology of avoidance and identification of Sybil attacks is implemented. In this proposed and implemented approach, the malicious node or selfish nodes are completely eliminated from the network, as the server agent takes full control of the ad-hoc network. By this method, there is reduced packet loss compared to the existing or classical approach of Sybil attacks. In this proposed approach, the packet loss is reduced to

Keywords – MANET Security, Sybil Attacks, Network Security

INTRODUCTION

Security and antivirus software is important for any network. One way security can break down is in a Sybil attack. Named after the case study of a woman with multiple personality disorder, a Sybil attack is a type of security threat when a node in a network claims multiple identities. Most networks, like a peer-to-peer network, rely on assumptions of identity, where each computer represents one identity. A Sybil attack happens when an insecure computer is hijacked to claim multiple identities. Problems arise when a reputation system (such as a file-sharing reputation on a torrent network) is tricked into thinking that an attacking computer has a disproportionally large influence. Similarly, an attacker with many identities can use them to act maliciously, by either stealing information or disrupting communication. It is important to recognize a Sybil attack and note its danger in order to protect yourself from being a target. First described by Microsoft researcher John Douceur, a Sybil attack relies on the fact that a network of computers cannot ensure that each unknown computing element is a distinct, physical computer. A number of authorities have attempted to establish the identity of computers on a network (or nodes) by using certification software such as VeriSign, employing IP addresses to identify nodes, requiring passwords and usernames, and so forth. However, impersonation, both in the real and digital worlds, is commonplace. Friends may share passwords, communities may share website registrations and some services provide a single IP address that is shared among users. Sybil attacks have appeared in many scenarios, with wide implications for security, safety and trust. For example, an internet poll can be rigged using multiple IP addresses to submit a large number of votes. Some companies have also used

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

Sybil attacks to gain better ratings on Google Page Rank. Reputation systems like eBay's have also been victims of this type of attack. There are few sure-fire ways to protect a network from a Sybil attack, but there is a wide range of literature dedicated to discussing options for protection and verification of computing identities. One way is by using trusted certification in which a single, central authority establishes and verifies each identity via a certificate. Trusted certification is not foolproof, however, and it can use up large amounts of resources and bottleneck traffic on the network. In this paper, the effective implementation of security against Sybil attacks is implemented with different parameters.

Mobile Ad-hoc Network (MANET) is defined as the moving node rather than any fixed infrastructure, act as a mobile router. These mobile routers are responsible for the network mobility. The history of mobile network begin after the invention of 802.11 or WiFi they are mostly used for connecting among themselves and for connecting to the internet via any fixed infrastructure. Vehicles like car, buses and trains equipped with router acts as nested Mobile Ad-hoc Network.

Vehicles today consists many embedded devices like build in routers, electronic devices like Sensors PDAs build in GPS, providing internet connection to it gives, information and infotainment to the users. These advances in MANET helps the vehicle to communicate with each other, at the time of emergency like accident, or during climatic changes like snow fall, and at the time of road block, this information will be informed to the nearby vehicles.

Nowadays technologies rising to provide efficiency to MANET users like providing enough storage space, as we all know the cloud computing is the next generation computing paradigm many researches are conducting experiments on Mobile Ad-hoc Network to provide the cloud service securely.

In case a mobile node wants to communicate with another mobile node which is too far from the source node, it should depend on relay node as bridge to communicate with destination. Relay node is nothing but another mobile node. In this case there arises a question of security. Apart from authentication, reliability and acceptance it should also aware of the address location and packet traffic digression.

SYBIL ATTACKS

The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder.

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

The name was suggested in or before 2002 by Brian Zill at Microsoft Research. The term "pseudospoofing" had previously been coined by L. Detweiler on the Cypherpunks mailing list and used in the literature on peer-to-peer systems for the same class of attacks prior to 2002, but this term did not gain as much influence as "Sybil attack".

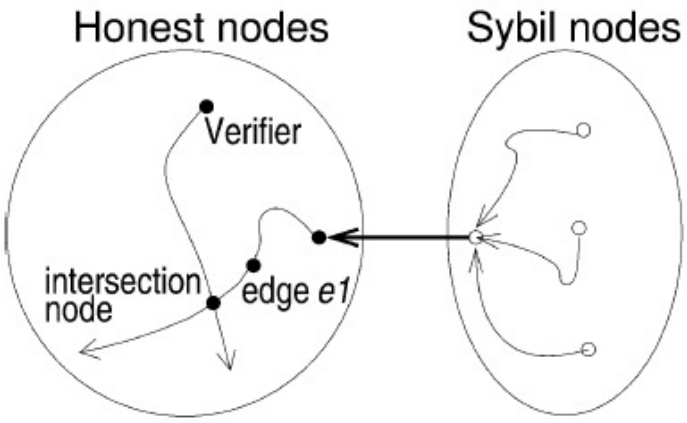

Figure 1 - Sybil and Honest Node

In a Sybil attack the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. Evidence shows large-scale Sybil attack can be carried out in a very cheap and efficient way in the realistic system like BitTorrent Mainline DHT.

An entity on a peer-to-peer network is a piece of software which has access to local resources. An entity advertises itself on the peer-to-peer network by presenting an identity. More than one identity can

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

correspond to a single entity. In other words the mapping of identities to entities is many to one. Entities in peer-to-peer networks use multiple identities for purposes of redundancy, resource sharing, reliability and integrity. In peer-to-peer networks the identity is used as an abstraction so that a remote entity can be aware of identities without necessarily knowing the correspondence of identities to local entities. By default, each distinct identity is usually assumed to correspond to a distinct local entity. In reality many identities may correspond to the same local entity.

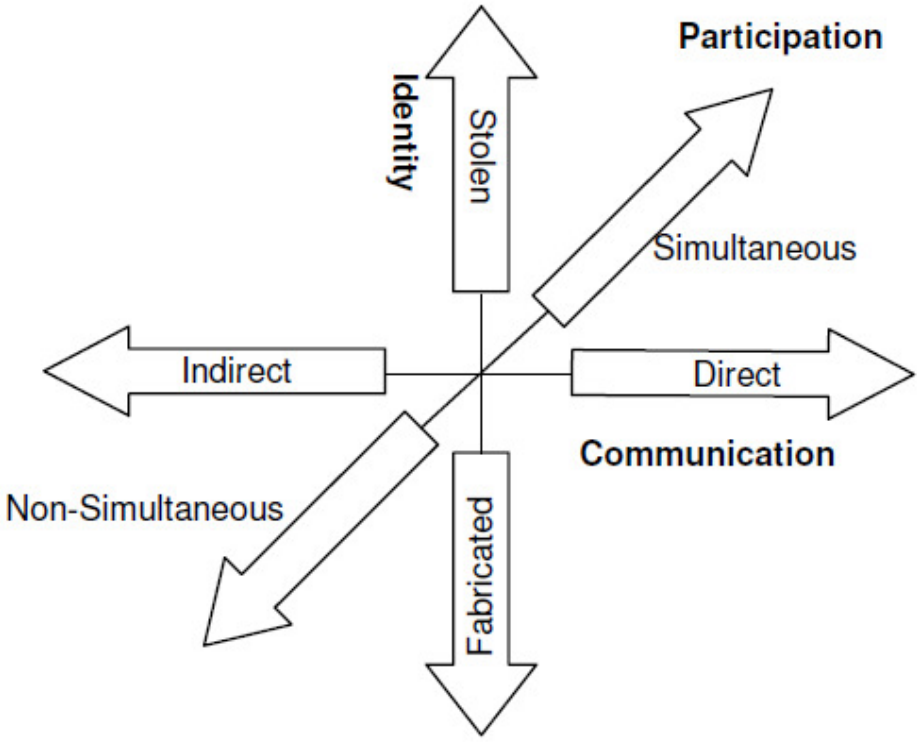

Figure 2 - Dimensions of Sybil Attacks

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

A faulty node or an adversary may present multiple identities to a peer-to-peer network in order to appear and function as multiple distinct nodes. After becoming part of the peer-to-peer network, the adversary may then overhear communications or act maliciously. By masquerading and presenting multiple identities, the adversary can control the network substantially.

In the context of (human) online communities, such multiple identities are known as sockpuppets.

Identity-based validation techniques generally provide accountability at the expense of anonymity, which can be an undesirable tradeoff especially in online forums that wish to permit censorship-free information exchange and open discussion of sensitive topics. A validation authority can attempt to preserve users' anonymity by refusing to perform reverse lookups, but this approach makes the Sybil prevention techniques based on the connectivity characteristics of social graphs can also limit the extent of damage that can be caused by a given sybil attacker while preserving anonymity, though these techniques cannot prevent sybil attacks entirely, and may be vulnerable to widespread small-scale sybil attacks. Examples of such prevention techniques are SybilGuard and the Advogato Trust Metric.

Validation techniques can be used to prevent Sybil attacks and dismiss masquerading hostile entities. A local entity may accept a remote identity based on a central authority which ensures a one-to-one correspondence between an identity and an entity and may even provide a reverse lookup. An identity may be validated either directly or indirectly. In direct validation the local entity queries the central authority to validate the remote identities. In indirect validation the local entity relies on already accepted identities which in turn vouch for the validity of the remote identity in question.

validation authority a prime target for attack. Alternatively, the authority can use some mechanism other than knowledge of a user's real identity - such as verification of an unidentified person's physical presence at a particular place and time - to enforce a one-to-one correspondence between online identities and real-world users.

SPECIFIC TYPES OF SYBIL ATTACKS

There are numerous malicious applications of Sybil attacks in different environments such as those including, but not limited to, the variations enlisted below.

Routing

Sybil attacks can disrupt routing protocols in ad hoc networks, especially the multicast routing

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

mechanism. Separate paths that initially seem disjoint may pass through the Sybil nodes of a single attacker. Another vulnerable concept is Geographical routing where malicious nodes may appear at more than one place at a time.

An attack in an ad hoc network and thus the availability of fake identities may further lead to a large scale attack such as distributed DoS, in addition to the inherently insecure routing protocols in such networks.

Tampering with Voting and Reputation Systems

In case of any environment where there is a voting scheme in place for purposes such as reporting and identifying node misbehaviour in the system, updating reputation scores and so on, a Sybil attack may be particularly dangerous. As an example, an attacker may create enough malicious identities to repeatedly report and subsequently remove legitimate nodes from the network. Alternatively, these malicious nodes can protect themselves from ever being removed as they are in collusion.

Fair Resource Allocation

Sybil attacks may also be used to enable the attacker to obtain an unfair and disproportionately large share of resources that were intended to be distributed amongst all nodes on the network equally. This attack denies legitimate nodes their deserved share of resources and also provides the malicious node with more avenues for other attacks.

Distributed Storage

File storage systems in peer-to-peer and wireless sensor networks can be compromised by the Sybil attack. This is achieved by defeating the fragmentation and replication processes in the file system. A system can be tricked into storing data into the multiple Sybil identities of the same node on the network.

Data Aggregation

Sensor network readings are computed by query protocols in a network rather than returning the reading of each individual sensor. This is done to conserve energy. Sybil identities may be able to report incorrect sensor readings thereby influencing the overall computed aggregate. A malicious user may be able to significantly alter the aggregate with enough identities.

PROPOSED APPROACH

Simulation Tools : ns2, xgraph, gnuplot
Platform : Red Hat Linux

This technique prevents the malicious node from attacking other nodes

1. *Allocation of the identification to the nodes*

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

2. *Source node request for the service*
3. *The server agent verifies the source ID, then it accepts the route request from sender then it gathers the information of receiver using destination ID from the list.*
4. *The server agent broadcasts RREQ using destination ID*
5. *The server agent select the adjacent node with the life time parameter*
6. *Server Agent gives RREP to source node, after this authentication process, source node sending data packets in a secure way.*
7. *Server Agent controls the mobile nodes and service requesting modules*
8. *The malicious node eliminated from the network because of non authentication*
9. *Logging of the Packets Loss*

COMPARISON GRAPH FOR THE PACKET LOSS

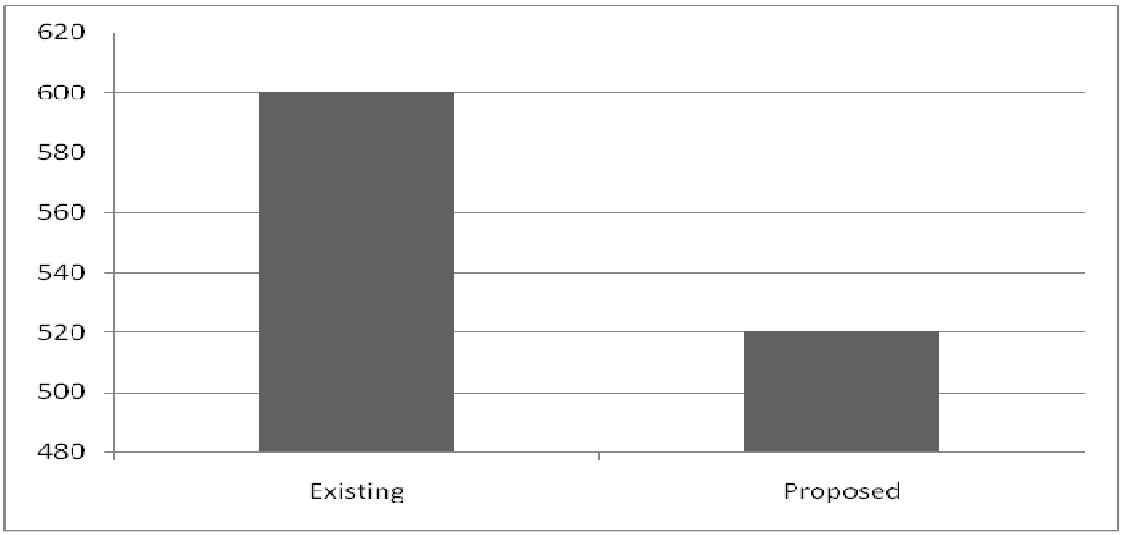

Figure 3 – Comparison Graph for Existing and Approach

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

Table 1 – Comparison for Existing and Approach

Packet Loss in the Existing Approach	600
Packet Loss in the Proposed Approach	520

CONCLUSION AND SCOPE FOR FUTURE WORK

This work center particularly on identification and evasion of Sybil assaults on the system framework whether it is concerned with the sniffing of bundles or taking the real recognize of the authentic hub. Nonetheless, there are number of procedures to address and evacuate this issue, yet our methodology is effective enough in light of the way that this proposed methodology is depending on the security trust building design. It implies there is a trust between the information transmission channel. The idea of versatile hub and server executors are coordinated to uproot any likelihood of the assault. In the proposed methodology execution, better brings about terms diverse parameters are gotten in distinctive recreation situations. For the future scope of the proposed work, the implementation of packet drop on every attempt of access by the intruder or attacker or unauthenticated node can be done. Using this methodology, the packet or signal will not be handed over to the non legitimate or unauthenticated node. In the future work, this work can be implemented to enhance the security.

REFERENCES

[1] T.H Clausen, “Introduction to Mobile Ad-hoc Networks (MANET)s” , 2007.

[2] “Wi-Fi (wireless networking technology)” published in encyclopaedia, 2002.

[3] Che-Fn Yu, “Security safe guards for intelligent networks”, GTE laboratories incorporated, 40 sylvan road, Waltham, MA 02254.

[4] V. Venkata Ramana, Dr. A. Rama Mohan Reddy, and Dr. K. Chandra Sekaran, “Bio Inspired Approach to Secure Routing in MANETs”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.4, July 2012

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

[5] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, IEEE, 2008.

[6] Tuna Guven, Hui Zeng, Jason H. Li, Song Luo, Subir Das, Tony McAuley, Thomas Stuhrmann, Joe Sherrick, Christine Adelfio, Seth Spoenlein, Aristides Staikos, Mario Gerla, "A Multi-Layer Approach For Seamless Handoff In Ad Hoc Networks With Wireless Heterogenity", IEEE, Paper ID 900668.pdf.

[7] D.Suresh kumar, K.Manikandan, M.A.Saleem Durai, "Secure On-Demand Routing Protocol for MANET using Genetic Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 19– No.8, April 2011.

[8] S. Prasad, Y.P.Singh, and C.S.Rai, " Swarm Based Intelligent Routing for MANETs", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[9] Poonam Garg, "A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April 2009

[10] Lu Han, Dongming Zhaow, and Manli Zhou, "A Network Layer Security Mechanism Based on Collaborative Intelligent Agents in MANET" IEEE,2005

[11] Santhosh Krishna B.V, Mrs.Vallikannu A.L, "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism", International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010

[12] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", international conference on wireless networks, 2003

[13] Marek Hejmo, Brian L. Mark, Member, IEEE, Charikleia Zouridaki, Student Member, IEEE, and Roshan K. Thomas, "Design and Analysis of a Denial-of-Service-Resistant Quality-of-Service Signaling Protocol for MANETs", IEEE Transactions On Vehicular Technology, Vol. 55, No. 3, May 2006

[14] Arif Sari and Dr. Beran Necat, "Securing Mobile Ad-Hoc Networks Against Jamming Attacks Through Unified Security Mechanism", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012

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

[16] Dimitris Mitropoulos and Diomidis Spinellis, "Securing e-voting against MITM attacks", 13th

ISSN (Online) : 2348 –2001
International Refereed Journal of Reviews and Research
International Refereed and Indexed Journal for Research Scholars and Practitioners

Volume 2 Issue 1 January - February 2014

International Manuscript ID – ISSN23482001V2I1012014M32

Panhellenic Conference on Informatics, Corfu, Greece, September 2009

[17] Latha Tamilselvan and Dr. V. Sankaranarayanan, "Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007

[18] Manel Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector Routing", Mobile Computing and Communications Review, Volume 6, Number 3.

[19] Dr. C. Anbalagan and Mr. T. Sugantha, "Implementation of Evolutionary Algorithms in Different Methods of Research- A Analytical Approach with Selection, Recombination, Mutation,

[20] Reinsertion and Population Model, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol.1, No. 1, October 2011

[21] Jason Leonard, "Interactive Game Scheduling With Genetic Algorithms", 1998

[22] Dr. James F. Smith III and Robert D. Rhyne II, "A Fuzzy Logic Algorithm For Optimal Allocation Of Distributed Resources".

[23] Manoj V, Mohammed Aaqib, Raghavendiran N and Vijayan R, "A Novel Security Framework Using Trust And Fuzzy Logic In Manet", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012