EXPLORATION OF SYBIL ATTACK REVELATION METHODS FOR PROTECTED DATA COMMUNICATION IN MOBILE NETWORK

V.Rajendhiran M.Vengadapathiraj K.Rajkumar M.Malarvizhi Dr.M.Saravanan

Mobile Netw

Abstract—**Mobile networks are made up of complex distributed systems that may also be part of a huge complex system. Due to this complexity of node, there is a need to develop more security solutions. Sybil attacks are one of the security threats to such complex networks. A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process in the network. Also one of the most important issues in mobile network is the secured data communication. There are various schemes to detect Sybil attacks with good accuracy in the presence of mobility also. In this paper, a secure node identification algorithm is proposed to detect the Sybil nodes also the pros and cons of various techniques to detect the Sybil attack is given. The various factors affecting the detection accuracy such as network contacts, packet transmission tariffs, node concentration, and node speed are also discussed. The proposed scheme can detect both join-and-leave and simultaneous Sybil attackers with the accuracy.**

Keywords—Sybil Attack, complex system, distributed systems, Identification, transmission rates.

I.INTRODUCTION

Many systems vulnerable to Sybil attack. The idea behind this attack is that a single malicious

Identity can present multiple identities, and thus gain control over part of the whole network. And then, the attacker can abuse the protocol in any way Possible. For instance he might gain responsibility for certain files and choose to pollute them. If the attacker can position his identities in a strategic way, the damage can be considerable. There might be possibility of an eclipse attack and slow down complete network by redirecting all queries in a false direction. Possibly carefully configured reputation-based systems might be able to slow the attack down, but it will not work more duration.

Peer-to-peer systems commonly rely on the existence of multiple, independent remote entities to mitigate the threat of hostile peers. Many systems replicate computational or storage tasks among numerousremote sites to defend against integrity violations (data loss). Others fragment tasks among several remote sites to protect against privacy violations (data leakage). In any case, abusing the idleness in the system necessitates the capability to regulate whether two apparently different remote entities are actually different.

Usage of the plural pronoun is regular even in solely authored research documents; however, assumed the subject of the current paper, its use herein is particularly ironic. If the local entity has no direct physical knowledge of remote objects, it observes them only as informational abstractions that we call identities. The system must ensure that distinctSelves refer to distinct stuffs; or else, when

ISSN: 2278 – 7798

the confined entity picks a subset of individualities to redundantly perform a remote operation.

II.THE SYBIL ATTACK

The Sybil attack has appeared in many forms in both academic work and in the real world. It is a severe and pervasive problem in many areas. Sybil attackers represent different identities of different target nodes. Consequently packets are directed to respective nodes can be redirected to the Sybil attacker. This result, Sybil attacker may drop all received packets. Sybil attacker also form loop by redirecting the received packet to those nodes which already in that packet. All identities of Sybil attacker are part of the same physical device and so they must situate in one area. All identities used by Sybil attacker is used as group of attack. A Sybil attack is also used by companies that increase the Google Page Rank rating of the pages of their customers, and Ease of Use has been used to link particular search terms to unexpected results for political commentary.Status systems are a common target for Sybil attacks including real-world systems like eBay.

III.GENERRAL METHODS

Since in the analysis of the Sybil attack, different approaches have been proposed to prevent or mitigate the attack. Approximately half of the published papers either suggest certification as a solution to the Sybil attack, following Douceur's approach, or simply state the problem without giving a solution. The remaining papers use distinct Strategies.

A. Trusted certification

Douceur has proven that trusted certification is the only approach that has the potential to completely eliminate Sybil attacks. Accordingly, it is cited as the most mutual solution. Though, reliable certification relies on a centralized ability that must ensure each entity is assigned exactly one identity, having certificate. But Douceur offers no method of ensuring such exclusivity, and in practice it must be performed by a manual or in-person process. If the enactment and security implications can be solved, then this approach can eliminate the Sybil attack

B. Radio resource testing

This method was proposed by Newsome for detecting Sybil attack in sensor networks. This is based on the assumption that each physical entity has only one radio resource and is able to transmit or receive only on one channel. Entity cannot transmit or receive message on more than one channel simultaneously. This approach is difficult to meet in VANET due to high mobility and impossibility of the pre deployment of the sharedinformation among Vehicles.

Each RRT is characterized by a set of parameters RRT (h, c, w) as follows. Parameter h is the size of the set $S = \{s_1, s2... sh\}$ of distinct identities that can be tested at the same time, in a solitary test.

IV. METHOD FOR PROPOSED STSTEM

A. Working:

A protocol have to be executed for provided that the security using identifier of node, which is created by using some secure algorithm. The security ensures the Accuracy of data, non-repudiation and substantiation

1. Forming Sybil Attack

In Sybil attack, a malevolent node acts as a Sybil which can whichevergenerate more than one identity on a single physical device in order to unveiling a synchronized attack on the network or can switch identities in order to weaken the Recognition processes in the network.

2. Proposed Plan:

In Proposed scheme utilizes the signal strength and header identifier of each node in order to differentiate between the legitimate and Sybil identities.

1) Demonstrate the entry and exit behaviour of legitimate nodes and Sybil nodes

2) Define a specific transmission range of packet that distinguish between the legitimate and Sybil identities based on nodes' entry and exit behaviour.

ISSN: 2278 – 7798

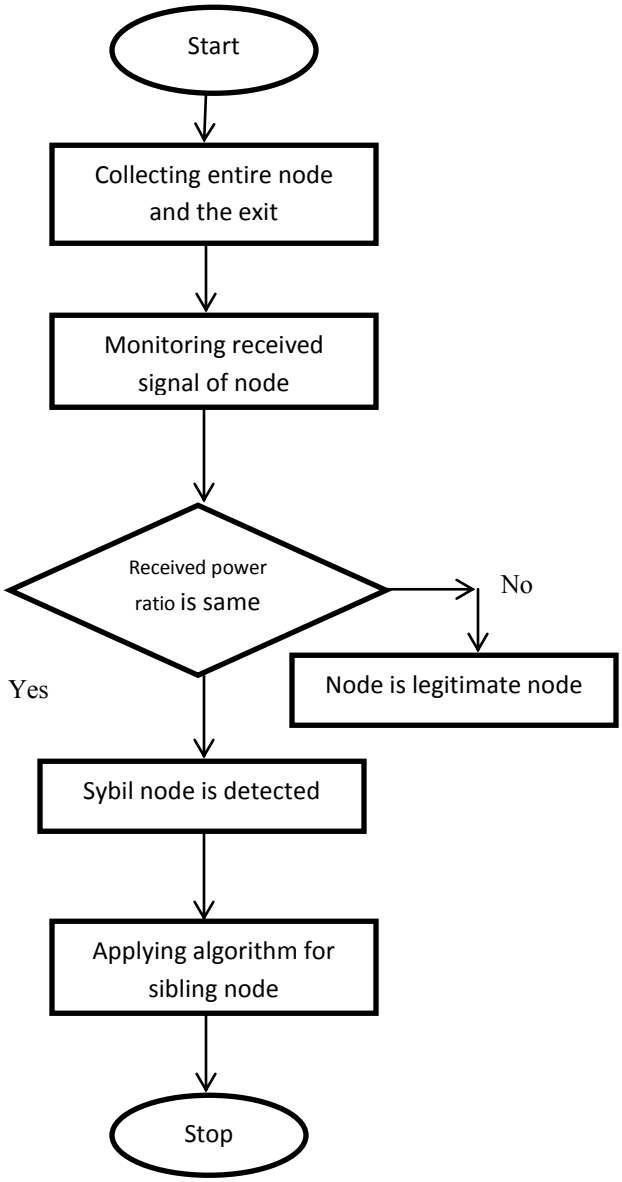

Figure 2: Flow chart of proposed plan

The first step consists of identifying features that distinguish Sybil nodes from honest nodes. The second step entails of acquiring and analysing a Sybil node, in which we search for behavioural attributes that may serve to identify them i.e. monitoring the received signal power of. This can be achieved using signal strengths of each node. As every node transmit and receive the signals while communicating. Third step, use the collected information to analyse the means and techniques used within Sybil's. More specially, it is possible to identify Sybil's, by analysing them consider it as Sybil or legitimate node which in the fourth step; and try to decrease the impact of these attacks by either injecting commands or disrupting the communication channel, block the Sybil node completely. In last step calculating the performance of network after and before the attack and Performance can be checked by using various parameter of the network such as throughput of the network and packet service ratio, energy consumption of network and end to end delay of network etc.

V. CONCLUSION

In This scheme, nodes share and manage identities of Sybil and non-Sybil nodes in distributed manner. The scheme can be applied to both scenarios of Sybil attacks.Whether the different identities are generated one after the other or all together both the case this method is useful. Also this scheme is work onvariable conveying power of node and work as a standalone scheme, but could similarly be deployed as an add-on to existing schemes, for case in point it could be combinedinterested in a reputation-based system.

REFERENCES

[1] B. Dutertre, S. Cheung, and J. Levy. Lightweight key management in wireless sensor networks by leveraging initial trust. Technical Report SRI-SDL-04-02, SRI International, 2002.

[2] P. Maniatis, D. S. H. Rosenthal, M. Roussopoulos, M. Baker, T. Giuli, and Y. Muliadi. Preserving peer replicas by rate-limited sampled voting. In Proc. ACM SOSP, pages 44-59, 2003.

[3] P. Maniatis, M. Roussopoulos, T. J. Giuli, D. S. H. Rosenthal, and M. Baker.The lockss peer-to-peer digital preservation system.ACM Trans. Compute. Syst., 23(1):2-50, 2005.

[4] B. Dragovic, E. Kotsovinos, S. Hand, and P. R. Pietzuch.Xenotrust: Event-based distributed trust

ISSN: 2278 – 7798

management. In Proc. Intl Wkshp on Database and Expert Systems Applications, 2003.

[5] J. Douceur. The Sybil Attack.In Proc. Intl Wkshp on Peer-to-Peer Systems (IPTPS), Mar. 2002.

[6] H. Rowaihy, W. Enck, P. McDaniel, and T. La Porta.Limiting Sybil attacks in structured p2p networks.In INFOCOM 2007.26th IEEE International Conference on Computer Communications. IEEE, pages 2596 {2600, may 2007}

[7] NitishBalachandran, SugataSanyal," A Review of Techniques to Mitigate Sybil Attacks", Int. J. Advanced Networking and Applications Volume: Issue: Pages.

[8] S. Buchegger and J. Le Boudec. A Robust Reputation System for P2P and Mobile Ad hoc Networks. In Proc. Wkshp Economics of Peer-to-Peer Systems, June 2004, 2002.

[9] Raya. M. And Hubaux," Securing vehicular ad hoc networks", Journal of Computer Security, 2007.

[10] Golle, P.Greene, D and Staddon, "Detecting and correcting malicious data in VANETs" In Proc of the 1st ACM international workshop on Vehicular ad hoc networks, 2004.

[11] Pal.S,Mukhopadhyay A.K and Bhattacharaya P.P, "Defending Mechanisms against Sybil Attack in Next Generation Mobil Ad hoc Networks", IEEE Technical Review, 2008.

[12] Nib B. Margolin and B. N. Levine. Quantifying and discouraging Sybil attacks. Computer Science Technical Report 2005-67, University of Massachusetts Amherst, Dec. 2005.

[13] B. Awerbuch and C. Scheideler. Group Spreading: A Protocol for Provably Secure Distributed Name Service. In Proc.Automata, Languages and Programming (ICALP), pages 183-195, 2004.

[14] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: analysis &defenses. In Proc. Intl Symp on Information Processing in Sensor Networks (IPSN), pages 259-268, 2004

[15] R. Rodrigues, B. Liskov, and L. Shrira.The design of a robust peer-to-peer system. In Proc. ACM SIGOPS European Wkshp, Sept. 2002.

[16] HimadriNathSaha ,Dr.Debika Bhattacharyya, An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 339 Volume 1, Issue 4, December 2010

[17] F. Cornelli, E. Damiani, and S. Samarati.Implementing areputation-aware gnutellaservent.In Proc. Intl Wkshp on Peer-to-Peer Computing, 2002.yal.

[18]J.H.Hartman, I.Murdock, T.Spalink, "TheSwarm Scalable Storage System", 19th ICDCS, 1999, pp. 74-81.

[19]ICANN, Internet Corporation for Assigned Names and Numbers, 4676 Admiralty Way, Suite 330, Marina del Rey, CA 90292-6601, www.icann.org.

[20]A. Juels, J. Brainard, "Client Puzzles: A Cryptographic Defense against Connection Depletion Attacks", NDSS '99, ISOC, 1999, pp. 151-165.

ISSN: 2278 – 7798