Incrimination Immune Method (I2M) – A Novel Messaging Technique To Combat Sybil Attack In Ad Hoc Network

First N. Sreenath, Second S. Vijayalakshmi, Third P.Annadurai

Abstract— **Ad hoc networks are an emerging area of mobile computing and efficient paradigm for infrastructure less communication. This paper analyzes the impact of Sybil attack with Incrimination Immune Method (I^2M). Sybil attack illegally claims/forges the identities of other genuine nodes in ad hoc network. The Master Sybil node maintains pool of subverted shadow identities which misuses them to disrupt the routing process. A malicious node incriminating or impersonating the other innocent nodes is defined as an entrap attack which forms a part of Sybil attack. The concept of Neighbor Aware Multicast Routing Protocol (NAMP) is deployed which warrants the creation of primary and secondary forwarding list. This idea has substantially helped the ad hoc network to be resilient to Sybil attack where a subverted node in the primary list disrupting the communication is blacklisted by the sender after receiving a threshold number of Node Accusation Report (NAR) from the genuine receivers which has bore the brunt of non receipt of packets. Consequently the Master Sybil node realizing the triviality of the shadow identities release them. These freed Sybil nodes jointly sends a unique novel message called Unleashed Sybil Incriminated Node Consensus Penalization (USINCP) to the sender in spotting the master Sybil adversary. This messaging technique is initiated only on demand (ie. When there is a Sybil attack) so it incurs less overhead and minimal memory requirements besides boosting the network performance. Two graphs have been theoretically conceived to study the effect of this messaging technique by plotting the number of groups with multicast members in x axis and end-to-end delay in y axis.**

Index Terms— **Ad hoc Network, NAMP, Node Accusation Report, Sybil Attack.**

I. Introduction

An ad hoc Network is built on the fly where a number of mobile nodes work in cooperation without the engagement of any centralized access point or any fixed infrastructure. Each host acts as a specialized router to relay information to other nodes. These autonomous mobile nodes communicate through a wireless medium in a multi hop fashion. The cooperation of intermediate nodes along the established route helps to forward packets on behalf of the neighbor to the destination node beyond the direct transmission range. Security has become a primary concern to provide protected communication between mobile nodes in a hostile environment.

Providing security support for mobile ad-hoc networks is challenging for several reasons: (a) wireless networks are susceptible to attacks ranging from passive eavesdropping to active interfering, occasional break-ins by adversaries (b) mobile users demand "anywhere, anytime" services; (c) a scalable solution is needed for a large-scale mobile network (d) Dynamic topology (e) infrastructure less (f) Peer –to-peer network (g) Lack of centralized authority [5]. Examples of applications for ad hoc networks range from military operations and emergency disaster relief to community networking and interaction among meeting attendees or students during a lecture [1].

The robust cooperative routing process becomes the cornerstone for network efficiency and performance. The routing process is vulnerable to an array of attacks which manifest itself in different gesture and stature. One such prominent attack is Sybil attack where malicious parties can compromise the network by generating and controlling large numbers of shadow identities. The shadow identities creates a permanent scar on the routing process by not forwarding the packet to the intended destination, pretending to forward and sending a fake acknowledgement, tamper the packet etc. The most destructive attack is the incrimination/entrap attack where the node with the shadow identity fabricates enough nefarious data about the captured identity and causes it to appear guilty and blacklisted thereby preventing its future occurrence in any routing path despite this being a genuine node.

A malicious node incriminating or impersonating the other innocent nodes is defined as an entrap attack. The objective of this paper is to define an Incrimination Immune Method (I^2M) which defends the shadow identities besieged by malicious parties from wrongfully exhibiting in the routing process. The Neighbor Aware Multicast Routing Protocol (NAMP) enables the creation of primary forwarding list (PFL) and secondary forwarding list (SFL) for route creation by source node using the Dominant Pruning method. The destination nodes are also in possession of these two lists. Any misbehavior exhibited along the PFL would automatically invoke the SFL of the source destination pair and the affected neighbor file a Node Accusation Report (NAR) about the shadow identities to the sender. The sender after receiving repeated accusation report of a particular node from various destination nodes blacklists the shadow identity.

F. N.Sreenath is with Pondicherry Engineering College, Pondicherry (e-mail: nsreenath@pec.edu).

S. S.Vijayalakshmi is with Pondicherry University, Pondicherry. She is now with the Department of Banking Technology. (Corresponding author Phone no: 9894597730; e-mail: anviji_lakshmi@yahoo.co.in).

T. P.Annadurai is with Kanchi Mamunivar College of Post Graduate Studies, Pondicherry (e-mail: annadurai_aps70@yahoo.com).

The blacklisted identities draw less attention during the routing process and appear less attractive than it was before blacklisting. The malicious party which has besieged the shadow identities releases them as it is resource less. The unleashed incriminated nodes collude with each other to penalize the Sybil adversary by a novel technique called USINCP (Unleashed Sybil Incriminated Node Consensus Penalization). The purpose of penalization is to append the offensive node in Corrupted Node List (CNL).

The organization of the paper is as follows. **Section 1** introduces the definition of the problem. **Section 2** highlights the Sybil attack and exemplifies the impact of Sybil Attack on Ad Hoc Network. **Section 3** expounds the NAMP. **Section 4** discusses the I^{2}M method which counters the Sybil Attack. **Section 5** presents results and discussion. Section **6** concludes the work with foreseeable enhancements.

II. Sybil Slowdown In Adhoc Network

A. Introduction to Sybil Attack

The Sybil attack is an attack by which a single entity can control a substantial fraction of the system by presenting multiple identities. The Sybil attack can be categorized into sub categories: (a) presentation of multiple identities simultaneously and exclusively (b) Fabricating new identities or duplicating the existing identities (c) Localized or globalized Sybil attack. Sybil attack can be perpetrated from network layer and application layer where the respective identifiers are IP address and Node ID. Sybil attack can defeat the objectives of distributed environment like fair resource allocation, voting, routing mechanism, distributed storage, misbehavior detection etc. The absence of logically central, trusted authority to vouch for a one-to-one correspondence between entity and identity promotes avenue for an unfamiliar entity to present more than one identity. Fig. 1 shows a conceptual view of Sybil attack.

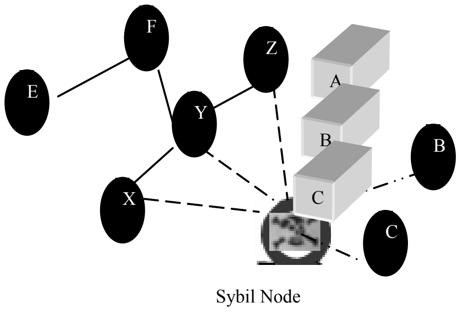


Fig 1: Sybil Attack.

B. General Security Concerns of Adhoc Network

Security is one of the most challenging issues in the field of communication networks. In case of MANETs, the challenge is escalated by the intrinsic properties of the ad-hoc communication scheme. Node autonomy and lack of centralized infrastructure require distributed and cooperative solutions for all functionalities implemented in MANETs including routing and data forwarding. This fact makes security a more challenging issue not only due to higher liability of the network to malicious activity, but also limits the possible solutions to the ones that do not require central control and infrastructure.

Malicious nodes may try to hide themselves and mimic natural uncertainties of the network to legitimize their malicious activity or try to run costly route discovery processes for unwanted and/or non existing destinations. The mobile nodes forward packets for each other, allowing communication among nodes outside wireless transmission range. The nodes' mobility and the fundamentally limited capacity of the wireless medium, together with wireless transmission effects such as attenuation, multipath propagation, and interference, combine to create significant challenges for routing protocols operating in an ad hoc network [2].

Attacks on ad hoc networks - Attacks on ad hoc network routing protocols generally fall into one of two categories:

- *Routing-disruption attacks.* The attacker attempts to cause legitimate data packets to be routed in dysfunctional ways.
- *Resource-consumption attacks*. The attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth or to consume node resources such as memory or computation power.

The most intractable difficulty is that a malicious node could incriminate and/or impersonate the other innocent nodes, which is defined as an *entrap attack*. This will endanger the trust relationship established among nodes and eventually disrupt legitimate network services. Ad hoc routing protocols are used to find an end-to-end path through the cooperative network. Each node needs a unique address to participate in the routing. Often addresses are assigned as an IP addresses or a unique Media Access Channel (MAC) address. Because all communications are conducted over the broadcast channel, these identifiers are available to determine what nodes are present in the network. In unsecured routing protocols, such as DSR or AODV, these address-based identifiers can be easily falsified by malicious nodes, which present an opportunity for a Sybil attack.

C. Sybil Shock in Adhoc Network

Consider the case where the attacker has at least 2 identities where one is false. In this case when a Sybil node receives a packet for a false identity it may: Drop/not forward the packet, alter the packet and attempt to send it as a legitimate forward, forward the packet to the false identity, impersonate that node and send an fake acknowledgement.

Ad hoc routing is a cooperative process, involving routers forwarding packets on behalf of other nodes. Sybil attack can manifest itself in routing disruption, resource consumption and packet dropping attack. A Sybil node can attack control messages corresponding to the route discovery, route activation and multicast tree management components of the routing protocol, or can attack data messages. Sybil node can prevent a route from being established by dropping the request and/or response, or can influence the route selection by using wireless specific attacks such as wormhole and flood rushing. It can also modify the packets carrying the route selection metric such as hop count or node identifiers. Sybil nodes can maliciously report that other links are broken or generate incorrect pruning messages resulting in correct nodes being disconnected from the network or tree partitioning [3, 4, 7, 8]

III. Review Of NAMP

This work discusses an efficient routing protocol for ad hoc network named as NAMP (Neighbor Aware Multicast Routing Protocol). NAMP aims at achieving higher performance by reducing control overhead and improvement of the end-to- end delivery of data packets. It is a tree based, hybrid multicast routing protocol. NAMP uses the neighboring information and dominant pruning approach for route creation.

Maintaining an established route is an important task. **As** any node can be drifted off from its current position at any time in ad hoc network, the routing protocol should also have the mechanism for maintaining this route. In this regard, NAMP applies the secondary forwarder list scheme. In dominant pruning approach, only efficient nodes are selected for forwarding the FLOOD-REQ packet throughout the whole network with minimum effort. The nodes that could be selected for flooding the FLOOD-REQ packet but was not selected by dominant pruning approach form the secondary forwarder list. Each node along the route has its own secondary forwarder list (SFL) and also sends the SFL to the selected forwarder. The selected forwarder node makes the nodes in the SFL know about the next forwarder node [5,6]. The notations used here are

○ — Source & Destination Node

● — Primary Forwarding List Node

▦ — Secondary Forwarding List Node

⊗ — Sybil Node & its Accomplice

→ — Primary Forwarding List

⇢ — Secondary Forwarding List

Fig. 2 to 7 illustrate the creation of PFL and SFL, subsequently the fail over mechanism incorporated by the subverted, incriminated Sybil node to nail the problem by deploying a unique messaging technique like USINCP and NAR.

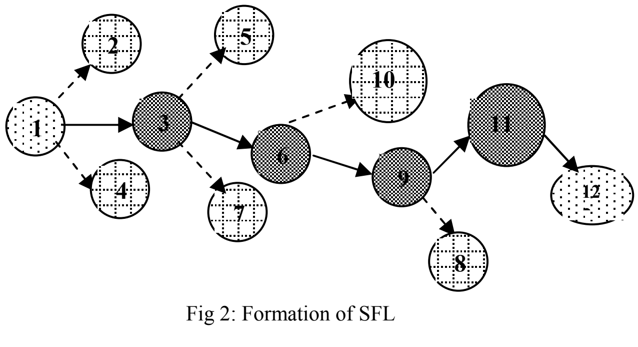


Fig 2: Formation of SFL

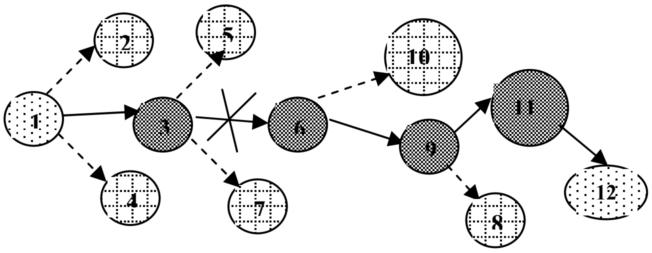


Figure 3: Failure of a link

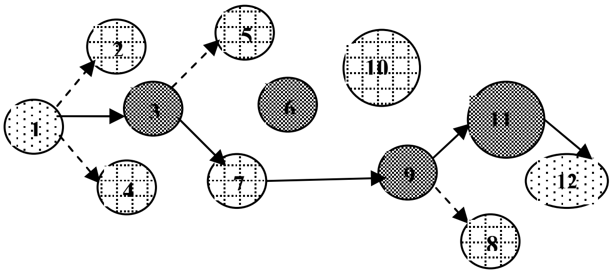


Fig 4: Route bypassing the faulty node

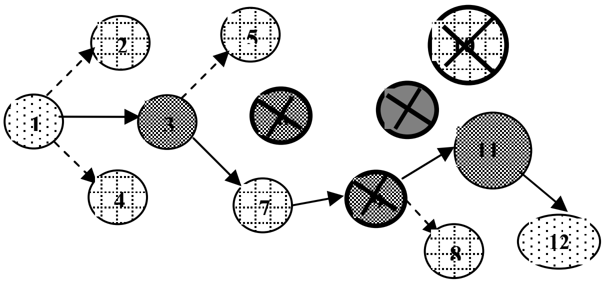


Fig 5: Manifestation of Sybil Attack

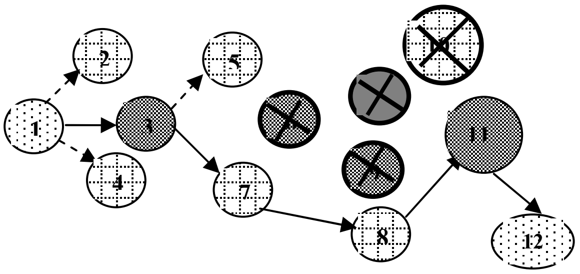


Fig 6: Route bypassing the Sybil Infected Node

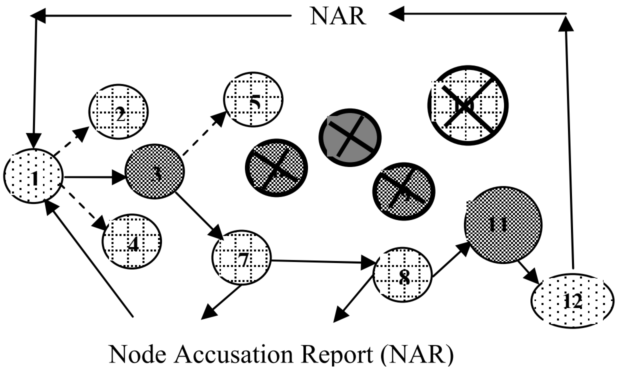


Fig 7: Neighbors Sending NAR & USINCP

IV. Incrimination Immune Method

NAMP routing protocol inherently advocates the creation of Primary Forwarding List (PFL) and Secondary Forwarding List (SFL) for the route discovery process. Any routing misbehavior exhibited by nodes along the primary route (PFL) would activate the nodes along the secondary route (SFL) to send negative acknowledgement signaling the non receipt of packets to the sender. Consider a malicious node illegitimately taking on multiple node identities which are labeled as Sybil nodes. The repercussion caused by the compromise of the last hop node by Sybil attack is of greater intensity and magnitude than the other civilian nodes. The sender after receiving a threshold number of negative acknowledgement from various destination nodes blacklist the Sybil nodes besieged by malicious adversary. The shrewd sender now routes the packet through a non faulty alternative forwarding path (SFL) that bypasses the Sybil nodes depriving them of their resource rich and promising status [6].

The incapacity exhibited by the then potential last hop node make them less promising and renders them liable for amputation from the established route. Malicious adversary that has duplicated the identities of these potential last hop nodes realizes the inefficiency of the nodes and checks them out from the pool of shadow identities. These stain free Sybil nodes join hands in unison in identifying and blacklisting the master adversary in the Corrupted Node List (CNL) maintained by the specific ad hoc network. These freed Sybil nodes refresh their key status to avert any capture in the future by any attacker and shoulder the onus of penalizing the Master Sybil adversary that has besieged them through a novel messaging technique called USINCP (Unleashed Sybil Incriminated Node Consensus Penalization)

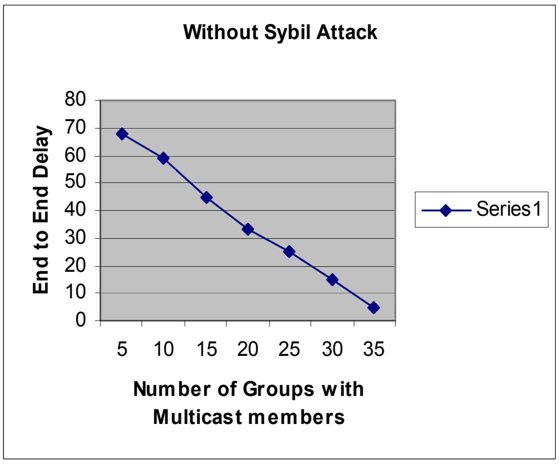
This type of blacklisting performed by the freed incriminated nodes is called Master blacklisting which inflicts a very severe blow to the Sybil attacker. This attacker which has jolted the network performance and throughput by duplicating the identities and disrupting the routing process is now at the sympathy of the Sybil Free Nodes. This technique incurs less overhead as NAMP protocol intrinsically warrants the creation of PFL and SFL. The throughput of the network though facing fluctuation in the initial phase stabilizes with the onset of this messaging technique and thus ensuring consistent performance. Storage and Computation complexities are absent in this messaging mechanism but it suffers from communication complexity as the created suspicion message has to effectively reach the sender. The maintenance of CNL helps the NAMP in avoiding the faulty nodes in the initial route selection process.

V. Results And Discussion

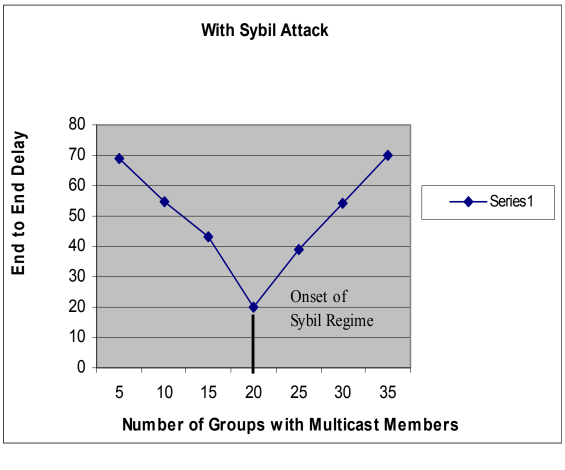
The after effects of the Sybil attack in ad hoc network are analyzed using end-to-end delay as the performance parameter. The NAMP inherently supporting the creation of two forwarding list namely the primary and secondary suffers from a switching delay if either of the list is corrupted or malfunctioning. The routing process juggle between these two lists. The corruption of the primary node by the Sybil adversary leads to the selection of secondary node for forwarding data to the destination. The less promising status of the Sybil infected nodes helps them to be released from the pool of shadow identities maintained by the Sybil attacker. These freed nodes in unison prosecute the master Sybil node by transmitting a novel messaging technique by name USINCP. There is obviously a delay in spotting the Sybil node which substantially increases the end-to-end delay of the packets being transmitted. The escalation in the delay parameter is attributed to several reasons (i) Creation and maintenance of two lists (ii) Hopping between the two lists if any of the nodes in these lists is corrupted or malfunctioning. (iii) Propagation delay of the unique messaging technique like USINCP which helps to identify the Sybil node.

Two graphs have been theoretically conceived to highlight the plight of Sybil infected routing process. The graphs are plotted with number of multicast group in the x-axis and end-to-end delay in the y-axis. The first graph shows the end-to-end delay value steadily decreasing after a robust and rigid route comprising primary and secondary route is computed in the absence of Sybil attacker. The second graph witnesses Inflation in delay value with the onset of black regime by Sybil attacker. The changing pattern in the delay value is attributed to the reasons mentioned above. The commencement of this USINCP messaging technique fairly reduces the end-to-end delay value after assaulting the Master Sybil Node.

A. *Without Sybil Attack*



B. *With Sybil Attack*



VI. Conclusion

This paper mainly focuses on the impact of Sybil attack on Mobile Ad hoc Network routing. Neighbor Awareness Multicast Routing Protocol (NAMP) is advocated which mandates the creation of PFL and SFL during the Route Discovery process. The two lists mutually extend support to each other when either of the forwarding nodes in any list is corrupted by Sybil attacker. Sybil attack substantially influences a part of the network by duplicating the genuine identities which is termed as entrap/incrimination attack. The neighbors of the Sybil infected node issue a suspicion message called Node Accusation Report (NAR) to the sender. The sender after receiving a threshold number of report trims the suspected nodes from the list making it less attractive to the Sybil adversaries thereby liberating the incriminated nodes. These unleashed Sybil infected nodes forward a Penalization message called USINCP (Unleashed Sybil Incriminated Node Consensus Penalization) about the adversary in unison to expel it to Corrupted Node List (CNL). This message in ad hoc network increases resilience to Sybil attack and is initiated only on demand (ie. When there is a Sybil attack) so it incurs less overhead and minimal memory requirements besides boosting the network performance which is echoed in Incrimination Immune Method (I^2M). The possibility of the nodes in the two lists being affected by Sybil adversary and simulation of this messaging technique in Network Simulator are the avenues for future enhancement.

References

[1] Varadharajan, V., Shankaran, R., and Hitchens, M., “Security for Cluster Based Ad Hoc Network”, Department of Computing, Information and Networked System Security Research, Elsevier Computer Communications, October 2004.

[2] Xu, S., “On the Security of Group Communication Schemes based on Symmetric key Cryptosystems”, Proc. of Conference on SASN, ACM, November 7, 2005, pp. 22 – 31.

[3] Besemann, C., Kawamura, S., and Rizzo, F., “Intrusion Detection System in Wireless Ad-Hoc Networks: Sybil Attack Detection and Others”, Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, October 4-7, 2004.

[4] Kefayati, M., Rabiee, R.H., “Misbehavior Resilient Multi Path Data Transmission in Mobile Ad Hoc Network”, SASN’06, October 30, 2006, Alexandria, Virginia, USA, ACM, 2006, pp. 259 – 268.

[5] Pathan, K.S.A., Alam, M., Monowar, M., and Rabbi, F., “An Efficient Routing Protocol for Mobile Ad Hoc Networks With Neighbor Awareness and Multicasting”, IEEE SECON 2004

[6] Hu, C.Y., Perrig, A., “A Survey of Secure Wireless Ad hoc Routing”, IEEE Computer Society, Nov.-Dec. 2006, pp. 12 – 23.

[7] Piro, C., Shields, C., and Levine, N.B., “Detecting the Sybil Attack in Mobile Ad Hoc Network”, IEEE Communication Surveys and Tutorials, Volume 7, No. 3, Third Quarter 2005, pp. 2 – 21.

[8] Lin, X., Zhu, H., Lin, B., Ho, P.H., and Shen, X., “A Novel Voting Mechanism for Compromised Node Revocation in Wireless Ad Hoc Networks”, IEEE Computer Society, 2006.

SREENATH.N is Head and Professor of Department of Computer Applications, Pondicherry Engineering College. He obtained his Ph.D (Optical Networks) from IIT-M and has completed M.Tech also. He has authored one research book and has written about 30 research papers in leading national and international journals. His research interests coincide with domains like High speed network, Optical networks, Information Security and Nano Sensors. Prof. Sreenath is on the editorial board of several reputed journals as well as in government committees.

VIJAYALAKSHMI.S is Lecturer of Computer science, Dept. of Banking Technology (School of Management), Pondicherry University. She is a Ph.D candidate currently doing research work on security in ad hoc networks. She holds M.C.A degree from SR College, Bharathidasan University, Trichirapalli and M.Phil degree from Alagappa University, Karaikudi. She has a teaching experience of 5 years in the field of Computer Science. She has authored 5 research papers which are published in refereed national and international journals and conferences.