Analysis of Sybil Impact on Network Life with Alert in Ad Hoc Communication

Nivodhaya. J, [1], Ramyadorai. D [2]

[1] PG Scholar, Dept OF CSE, ACE, Hosur, Tamilnadu, India,
[2]Associate Professor, Dept OF CSE, ACE, Hosur, Tamilnadu, India,

Abstract

This paper proposes the study result of the energy level depletion in an geographic anonymous routing protocol ALERT [1] due to Sybil attack. The Mobile Ad Hoc Networks (MANETs) for hostile environment requires secure and stable setup. Anonymous routing strategy which hides the routing information from the outsiders can provide highly secure communication among mobile nodes but cannot guarantee the stability of the network. Highly Secure network along with longer lifetime is the need of the hour for critical environments. Increasing the residual energy of the network indirectly increases its lifetime. Energy conservation in the network can also be achieved by mitigating the effects of the attacks that are aimed at the depletion of the nodal energy directly and network energy indirectly. Sybil attack is one of the well-known effects for such energy drain. The proposed work is aimed at studying the effect of Sybil attack [2] with network energy in ALERT (Anonymous Location based Efficient Routing)[2]. Extensive simulations are done by inducing Sybil entities in ALERT routing and the results prove that the conservative network energy level decreases considerably with Sybil nodes.

***Index Terms:** Mobile ad hoc networks, Anonymous routing, Sybil attack.*

---***---

1. INTRODUCTION

Mobile ad hoc networks are the self-organizing and self-adaptive networking solution for the environments where the classical networking infrastructure cannot withstand. Such an network does not involve any central authority for its control and monitoring. This nature makes them more vulnerable to the attacks that are imposed on the security of the communication information. Hence Anonymous kind of routing strategy that hides the information on the core process like routing, computing etc. is the need of the hour for the secure communication.

Ad hoc networking for the hostile environment demands both security and stability for their prolonged usage. Therefore efficient utilization of mobile node's battery power is very important because frequent recharging of mobile nodes may not be an easy and not possible task for situation like hostile and critical environment. Even anonymous routing all alone cannot guarantee the stability of the network. Stability indeed is related to the lifetime of the network. Network lifetime is one of the vital concerns for the successful deployment of the network in critical environments like battlefields.

Network lifetime for mobile networking is related to the energy level of the mobile nodes and its optimal usage maximizes the nodal lifetime directly and the network lifetime indirectly. Conservative energy depletion of network can happen with some attack that causes unusual energy consumption. One such attack is the Sybil attack that creates faulty identities and tends to create high rate of duplicate traffic among nodes which will drain the energy of the mobile nodes and residual energy of overall network. This causes reduction in the lifetime of the network. The proposed work is aimed at analyzing the impact on energy level due to the Sybil attack [2] in low cost anonymous routing protocol ALERT[1].

The proposed simulation study will provide better insight about Sybil attack in ALERT and such that one can develop better Sybil protection algorithm for ALERT protocol.

2. ROUTING MECHANISM IN ALERT

Several Anonymous routing protocols proposed in the literature uses either high cost solutions for providing anonymity in routing by implementing redundant traffic [3-9] or hop by hop encryption mechanism [10-14]. These protocols provide anonymity protection either to the data sources (sender and receiver) or to the route of the communication but not both [2]. Moreover high cost solution cannot be beneficial for the scalable networking [15]. ALERT is capable of providing anonymity protection for the data sources and route and incur low cost solution as well. Hence ALERT [1] can be the beneficial solution for hostile ad hoc networking.

ALERT mechanism involves dynamic partitioning of the zone such that the sender and the destination zone are separate. Once the partition is made, a random location is selected in the other zone and the node closer to the random location is chosen as the random forwarder. Then the packets are transferred to the random forwarder using the GPSR[16] algorithm. H denotes the total number of partitions made and is calculated as:

$$H = \log_2 \frac{\rho . G}{k} \qquad \text{-------} \ (1)$$

Where, ρ is the density of network, G is the size of the network area and k is the number of nodes in the destination zone.

The entire network area is a rectangle with side lengths lA and lB and the entire area is partitioned H times to produce a k anonymity destination zone. ALERT uses the two functions for finding the two side lengths of the hth partition:

$$a(h,l_A) = \frac{l_A}{2^{\lceil h/2 \rceil}} \qquad \text{-------} \ (2)$$

$$b(h,l_B) = \frac{l_B}{2^{\lceil h/2 \rceil}} \qquad \text{-------} \ (3)$$

The side lengths of the destination zone after H partitions are $a(H,l_A)$ and $b(H,l_B)$.

Fig.1 shows an example of three partitions of the entire network area. The side lengths of the final zone after the three partitions are shown in Fig -1.

Symmetric cryptographic techniques are used in place of high cost public key cryptography to offer cheaper solution [17]. ALERT is highly resilient to the intersection and timing attack by implementing “notify and go” mechanism.

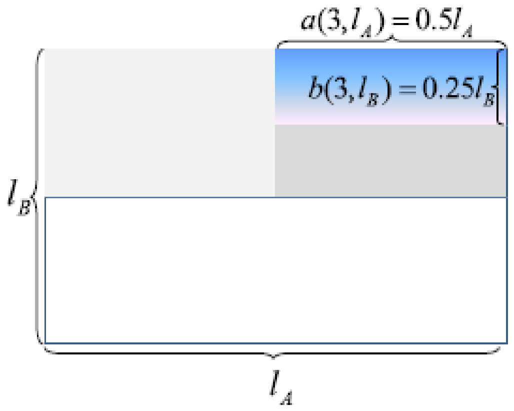

Fig -1: The side lengths of third zone

3. ENERGY ANALYSIS ON ALERT

The greedy forwarding in ALERT to the random forwarder do not consider the inherent battery power of the node on the route. In case of simultaneous communication between same pair of nodes, the node which is immobile for a longer time and being closer to the destination is chosen always as the forwarding node and causes battery drain in such nodes leading to network failure or partition. The figure describes the scenario of nodal drain out.

Another case is when there are nodes with fractional difference in distance from the destination; the greedy forwarding always chooses the closest node. This causes unfair usage of nodal energy even with fractional difference in distances. Thus unfair nodal energy depletion and drain out may happen with ALERT routing.

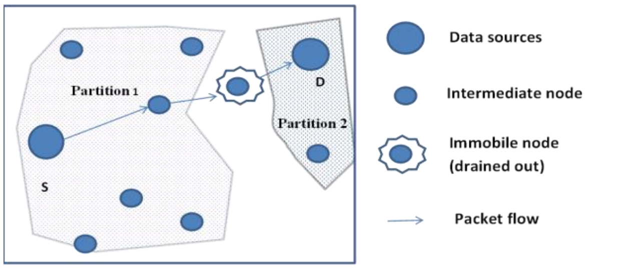

Fig -2: Network partitioning due to nodal drain

The usage of pseudonym in ALERT imposes the chance for active attacks [13] into the network. Sybil attack is an attack that creates duplicate identity for nodes. This violates the one to one mapping of the nodal identity in vehicular ad hoc networks the Sybil identities are more predominant as they create fake registry for vehicles and causes traffic collision and mesh [18]. Sybil entities are also capable of disrupting geographic based and multipath routing [19]. The most vital requirement of MANET is the distinct, unique and persistent identity per node for the protocols to be viable [19].

4. SYBIL ATTACK ON NETWORK LIFETIME

Sybil nodes have great impact on energy consumption in a network. The needful energy in the network is used by the Sybil nodes for sending and computation of duplicate notification messages about their presence. In applications like battle fields, the intended Sybil node can focus on the commander node and can deplete its battery power by continuously sending duplicate messages as the node should use some power for the reception and computation of the messages. Fig -3 below depicts the case of the draining out of such critical node

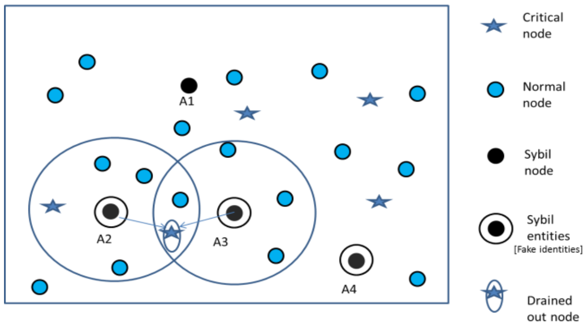

Fig -3: Sybil impact on nodal power

ALERT is vulnerable to the Sybil attack due to the usage of the pseudonym for nodal identity. A node in ALERT can create more than one pseudonym and depict as distinct nodes. Such an attack can cause reduction in the network energy level and thus reduces the network lifetime. This imposes danger on the stability of the network when applied in critical situations.

5. SIMULATION WORK

Simulation for the proposed work is carried out with the familiar network simulator NS2. Table 1 defines the details of the simulation work.

Table 1 : Simulation parameters

Parameter	Level
Examined Protocol	ALERT
Simulator	NS-2
Simulation time	250 sec
Simulation area	1000 x1000m
Number of nodes	100
Number of identities per Sybil node	1
Mobility model	Random waypoint model
Number of base stations	1
Transmission range	250m
MAC	802.11
Application	CBR
Packet size	512 bytes
Initial energy	1000 J

The simulation is carried out by inducing 1, 5, 10, 20, 24 Sybil nodes and is noted that the residual energy level in network is respectively. Initially the energy level in the network after the transmission without any Sybil entity is J.

6. RESULTS AND DISCUSSION

The results of the simulation were analyzed and tabulated in Table 2. Table below shows the energy in the network with and without Sybil entities.

Table 2 : Simulation parameters

Number of Sybil attack node	Energy Level in 100 nodes (J)	Energy loss from initial %	Energy loss due to Sybil %
0	822	17.8	0.0
1	817	18.3	0.6
5	742	25.8	9.7
10	643	35.7	21.8
20	521	47.9	36.6
24	453	54.7	44.9

The energy level depletion in the network is considerable. The Sybil attack with ALERT decreases the network lifetime. The lifetime of the ad hoc network with critical environments needs longer lifetime. Hence the mechanism for detection of Sybil with the considered protocol could increase the network life in the hostile deployment of such networking.

7. CONCLUSION AND FUTURE WORK

The work in the paper is the study result of the energy level depletion in the ad hoc network with the low cost anonymous routing protocol ALERT due to the Sybil attacker nodes. The simulation results are evident to prove the considerable depletion in the residual energy of the network due to the Sybil nodes and is calculated to be more than the Sybil free network. The future work is aimed at studying the energy conservation in ALERT with the energy aware mechanism considering the inherent battery power of the forwarding nodes along with the distance parameter and the impact of Sybil attack on such a scenario.

REFERENCES

[1] Haiying Shen, Lianyu Zhao, ”ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs”, IEEE Transactions on Mobile Computing , vol 12 June 2013.

[2] J. R. Douceur, “The Sybil attack,” presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.

[3]Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,” Wireless Networks, vol. 11, pp. 21-38, 2005.

[4] I. Aad, C. Castelluccia, and J. Hubaux, “Packet Coding for Strong Anonymity in Ad Hoc Networks,” Proc. Securecomm and Workshops, 2006.

[5] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, “An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks,” IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[6] X. Wu, “AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol,” IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.

[7] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, “Anonymous Secure Routing in Mobile Ad-Hoc Networks,” Proc. IEEE 29th Ann. Int’l Conf. Local Computer Networks (LCN), 2004.

[8] A.R. Beresford and F. Stajano, “Mix Zones: User Privacy in Location-Aware Services,” Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW), 2004.

[9] X. Wu, J. Liu, X. Hong, and E. Bertino, “Anonymous Geo- Forwarding in MANETs through Location Cloaking,” IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.

[10]Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, “An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks,” Proc. Int’l Symp. Applications on Internet (SAINT), 2006.

[11] Z. Zhi and Y.K. Choong, “Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy,” Proc. Third Int’l Workshop Mobile Distributed Computing (ICDCSW), 2005.

[12] V. Pathak, D. Yao, and L. Iftode, “Securing Location Aware Services over VANET Using Geographical Secure Path Routing,” Proc. IEEE Int’l Conf. Vehicular Electronics and safety (ICVES), 2008.

[13] K.E. Defrawy and G. Tsudik, “ALARM: Anonymous Location- Aided Routing in Suspicious MANETs,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2007.

[14] K.E. Defrawy and G. Tsudik, “PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs),” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2008.

[15] Lianyu Zhao, ”A low cost anonymous routing protocol in MANETs” ICCCN 2009

[16] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, “Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table,” Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.

[17] Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.

[18] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in Proc. 4th Workshop HotNets, 2005, pp. 1–6.

[19] “Lightweight Sybil Attack Detection in MANETs” , Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat , IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013.