2012 International Conference on Indoor Positioning and Indoor Navigation, 13-15th November 2012

Efficient, Authentication and Access control Implementation in Mobile Ad hoc Networks (MANET) as applied to Indoor Navigation Guidance System for Vision Impaired People

Prabath Lakmal Rupasinghe
Department of Electrical and
Computer Engineering
Curtin University
Perth, Western Australia
p.rupasinghe@postgrad.curtin.edu.au

Nimsiri Abhayasinghe
Department of Electrical and
Computer Engineering
Curtin University
Perth, Western Australia
kahala.abhayasinghe@postgrad.curtin.edu.au

Iain Murray
Department of Electrical and
Computer Engineering
Curtin University
Perth, Western Australia
I.Murray@curtin.edu.au

***Abstract*— Indoor navigation systems are becoming increasingly popular. Blind and Low Vision users are prominently in need of indoor positioning and navigating systems as indoor navigation is a significant issue. Most of the efforts in creating such systems are using MANET (Mobile Ad-hoc Networks) as the base technology. However the properties of MANET's inherently provide greater challenges in areas like security, reliability and performance. Most of research work was done on those different challenges in isolation. A holistic approach to address all these challenges in an implementation appears to be rare.**

Ad-hoc collaboration is usually an unplanned interaction or created "immediately on the fly". In MANET networks Authentication and access-control trust relations established through, on-line- available evidence, may be short-term and largely peer-to-peer, where the peers may not necessarily have a relevant network that can be placed into a recognizable trust hierarchy. Trust relations involving a captured node need to be invalidated, and new trust evidence need to be collected and evaluated to maintain node connectivity in the ad-hoc network This paper present the framework on Trust Relations based on friendships mechanism which is adopted from the theory of small-world phenomenon (i.e. six degrees of separation) initiated by Milgram, to provide rapid authentication.

Continuity Efficient, Rapid Authentication is needed in practical implementations of an Indoor navigation system. Particularly when Low vision users are dependent on such system, a rogue node can be hazardous. Further research delivers a framework which combines reliability and performance, two important factors in practical implementation of an indoor navigation system.

KEYWORDS: MANET, Vision Impaired, Indoor Navigation, Authentication, Trust

I. Introduction

In recent years, network security has received critical attention from both academia and industry. As the data network becomes more pervasive and its scale becomes larger, network intrusion and attack have become severe threats to network users. This is especially true for the emerging wireless data networks. Compared to their wired counterpart, wireless networks are prone to security attacks ranging from passive eavesdropping to active interfering. As it is even more difficult to protect network entities against the intruders in wireless environment, occasional break-ins in a large-scale mobile network are nearly inevitable over a large time period. In Ad hoc networking this threat becomes greater.

Ad hoc networking is where potential mobile users arrive within the common perimeter of radio link and participate in setting up the network topology for communication. Nodes within the Ad-hoc network communicate through wireless links or multi-hop routing without any infrastructure setup [1]. Practical situation like indoor navigation system for Vision impaired people is highly dependent on Mobile Ad hoc networks which are the area of discussion in this research. In terms the security of these networks are in stake, ultimately making the users vulnerable.

It's obvious that with lack of infrastructural support and susceptible wireless link attacks, security in Ad-hoc network becomes inherent weakness. Achieving security within Ad-hoc networking is challenging due to following reasons [3,4], first the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering. Second the lack of online CA (Certificate Authority) or Trusted Third Party adds the difficulty to deploy security mechanisms. Additionally mobile devices tend to have limited battery life and computation abilities which make it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms. Next, MANETs there are more probabilities for trusted mode being compromised and the being used by adversary to launch attacks on networks, in other word; we need to consider both insider attacks and outsider attacks in MANETs, in which insider attacks are more difficult to deal with. Finally Node mobility enforces frequent networking reconfiguration which created greater opportunities for attacks, for example, it is difficult to distinguish between stale routing information and faked routing information.

This paper proposes a mechanism to mitigate the problem of having insecure nodes in MANET known as the Cluster-Friend mechanism that is adopted from the theory of small-world phenomenon to encourage trustworthiness among nodes in a trusted environment. Mechanism will focus on using cluster based routing protocols.

II. Background

The work is a part of a larger project that is developing an indoor navigation system for vision impaired people using mobile devices such as smart phones and tablets. The following sections describe the related literature.

A. Current Litreature

Most of the current research work on security in Ad Hoc Networking falls in encryption, secure routing, quality of service etc. Each of them is designed to operate in a particular situation, which may fail to work successfully in other scenarios.

The supported routing protocols within ad hoc network are more vulnerable to attacks as each device acts as a relay [1]. Any tampering with routing information can compromise whole network. An attacker can insert rogue information within routing information or introduce denial of service type attack by replaying old logged or stored information. Also compromised node can route malicious information to other nodes, which can cause serious damage. However proposed routing solutions are capable to operate with dynamic topology but in terms of security measure [2] they provide partial or no solution [2]. Thus implementation of secure routing protocol is one of the challenges within ad hoc network.

The problem of Authentication and access control in Ad hoc networks has received very little attention. Existing solutions assume that messages sent can be accessed by all Nodes in the vicinity. Group based approach has also been taken in CARAVAN [2] and AMOEBA [3]. Nodes moving together belong to one group. Any member can sign a message using a group signature scheme and the others can verify it even without knowing the identity of the signer. However, the election of leaders (to assign group keys), and the fast changing groups (due to ephemeral nature of the network) make it difficult in practical situations

Several works have been carried out to overcome the problems of selfish nodes in MANET environment. In the work done by Marti et al. [6], they use a watchdog mechanism to detect selfish nodes and path rater mechanism to avoid them. Their work has managed to increase network throughput but those mechanisms cannot cope with the selfish nodes effectively as they do not penalized any misbehaving nodes.

B. Small-world Phenomenon

In this section, Cluster friendships mechanisms are discussed as a method to motivate high cooperation among nodes in a MANET environment. This friendships mechanism is adopted from the theory of small-world phenomenon (i.e. six degrees of separation) initiated by Milgram [5]. Milgram suggested that any two individuals in this world are likely to be connected through a short sequence of no more than six intermediate acquaintances.

The small-world problem has become a popular cultural phenomenon, especially after the playwright Guare [4] chose the term six degrees of separation as the title of his play. Milgram together with his graduate student Jeffrey Travers devised an experiment to test the small-world problem. Milgram gave 300 letters to participants in Boston and Omaha, along with instructions to deliver them to one particular target person by mailing the letter to an acquaintance they considered to be closer to the target. That person then got the same set of instructions, which therefore, set up a chain of intermediaries. Authors found that the average length of these chains was about six, which reveal the fact that human society in this world is actually bounded in shorter path lengths than would generally be thought.

Currently, there is only few implementation efforts of Milgram's small-world phenomenon theory in MANET. One of the interesting of Milgram's theory in MANET was done by Razak [6]. The research attempted to mitigate the problem of uncooperative nodes in ad hoc network by adapting the concept of trust chain through friends' recommendations. It is believed that everyone has a set of friends that an individual can trust or distrust. The question of how the trust relationship is developed is not an issue in this study; the focus is rather given to establish initial trust with everyone's sets of friends.

For an example, A has two friends B and C. A also has another friend D who A trusts so much. B and C have never met D before but due to A's recommendation on D to B and C, D is also now become friend to B and C who share the same level of trust as A. The process of recommending trust continues until each person reaches the maximum level of the sixth degrees of friends.

Further Watts and Steve [7] showed the theoretical description and analysis on the small world network, which is neither completely regular nor completely random, but a case between these two extremes. Kleinberg [8] proposes a theoretical framework for analyzing graphs with small world properties. His work reveals that the small world model has two fundamental components: first short chains exist ubiquitously, and second individuals operating with purely local information are very adept at finding these chains.

SW-R2P, a trusted small world overlay P2P(Peer-to-Peer) network with role based and reputation based access control policies, in order to implement efficiency and security Peer-to-Peer network was proposed by Xia et al.[9] .

All the work above focuses on the small world topology used to solve P2P issues, such as robustness, hop length and reliability. Similarly, there is also some research concerning on small world topology in ad hoc networks. However, all the research work above focuses on the feasibility, efficiency and robustness, ignoring the trust issues which should be such an important concern in ad hoc networks.

In this paper, our model considers the trust issue with Rapid Authentication in mind. The idea of friends' recommendation and trust sharing of this study are applied in MANET to increase the nodes' cooperativeness in network operations of a trusted community.

III. Proposed Method

According to the small-world concept the trust can be developed in the ad hoc network by allowing the node owners to participate in trust creation to the network. This condition comes with the assumption that all trusted nodes will have rapid authentication without any protocols because all involving nodes have greater trustworthiness with each other.

This research uses a novel approach by adapting friendships mechanism with clusters. It has been shown that MANETs based on ''flat'' routing schemes, such as Fisheye State Routing (FSR) [10], Ad Hoc On-demand Distance Vector Routing (AODV) [11] and Dynamic Source Routing (DSR) [12], cannot perform well when the network size increases, especially in face of node mobility as well, due to link and processing overhead [13]. A more common way to solve this scalability problem is hierarchical routing [13]. A typical way to build hierarchy is to group mobile nodes geographically near to each other into explicit clusters and assign different functionalities to mobile nodes inside and outside a cluster [14].

A cluster-based routing scheme consists of two major parts: the clustering algorithm and the routing algorithm. The clustering scheme discusses how to form and maintain a cluster structure in a dynamic MANET. The routing scheme discusses how to discover and maintain routes on the top of the cluster structure. Two typical cluster based routing schemes are Clusterhead-Gateway Switch Routing (CGSR) [16] and Cluster based Routing Protocol (CBRP) [15].

Research uses cluster structure proposed by CBRP Routing protocol [15]. Mobile nodes may have different cluster-related status or function, such as clusterhead (CH), clustermember (CM) and clustergateway (CGW). A mobile node selected as a CH serves as the local coordinator for its cluster, and its ID is usually utilized to identify the corresponding cluster A CGW is a non-CH node that either belongs to two or more different clusters or can directly connect to some non-CH node residing in a different cluster. A CM is a non-CH node of a cluster without any inter-cluster links.

In the proposed method cluster would be created with trusted nodes. Hence nodes are allowed to forward packets only among trusted nodes in the cluster. As for that, nodes will not going to communicate with other anonymous nodes that are not in the cluster as they are bounded in the friendships mechanism policy.

Suppose two clusters needed to be connected together, hence a node will find which resides in two or more clusters which acts as CGW (Cluster Gateway). These nodes will be trusted by connected clusters due to the being in [6] the same group of friends.

Next in small world network implementation is to determine the Trust probability (Tp) connecting different CGWs. Tp is based on prefetched trust knowledge through friendship. They have different scales which need to be mapped to a consistent range.

$$Tp = F(w1\ f1(x1) + w2\ f2\ (x2\ ) + w3\ f3\ (x3\ ))$$

CGW should build a link of other nodes (Authenticated Route) by looking at the Tp values. Choosing proper nodes to build a proper route expands the scale of small world network. The CGW will calculate the probability Tp based on its perfected knowledge, and decide the Authenticated route information connecting to other clusters. Different f1, f2, f3 functions provide criteria to define the trust level in each CGW.

When a new node joins one of the clusters in the network, it is necessary to determine its role in the cluster, CH, CM or CGW node. We will show criteria for the cluster to choose the clusterhead and clustergateway. The criterion is used to judge whether the node can afford to play the role as the head nodes based on its Trust and other properties. The criterion function is as following:

$$T(node)=w1*Enc(node)+w2*Pow(node)+w3*Range(node)+w4*InitTrust(node)$$

In this function, T() is the overall evaluation for a node, and w1, w2, w3, w4 are weights for different concerns. These weight values will be set by the level of trust within friend relationships. The Enc () represents the node's Encryption capability. The trust level depends on the encryption ability or type of key being used. The better encryption type is used, the higher the level of trust will be given. The Pow() is the Battery power of the nodes and the Range() is the maximum range that the node can reach. InitTrust() use of discrete values to denote the initial trust levels of a node from complete distrust to complete trust. The values are related to the types of trust relationships of the friends in the cluster.

As following the function above, the original ad hoc network may gradually evolve to a small world ad hoc network. Furthermore, to achieve the Authentication ware small world implementation, we still need to design specific protocols about the action on the nodes and links.

IV. Conclusions

With the cluster structure, the processing and spreading of routing information are restricted to partial mobile nodes in the network based on their cluster status. Mobile nodes that participate in routing in such cluster-based routing are called routing backbone nodes, and normally CHs and CGWs serve as the routing backbone nodes. In other words, the cluster structure can help reduce the routing space (referring to the number of routing backbone nodes) and the routing overheads without affecting the routing efficiency. Hence, cluster-based routing connected with trust mechanism should be able to provide better efficient authentication solutions for MANETs.

References

[1] L. Zhou and Z.J. Haas, "Securing Ah Hoc Networks", IEEE Networks, 13(6):24-30, Nov/Dec 1999

[2]. Sampigethaya, K.,Li, M., Huang, L., Li, M., Poovendran, R., Matsuura, K., Sezaki, K.: Caravan:Providing Location privacy for vanet. In: Proc. of the Workshop on Embedded Security in Cars, ESCAR(2005)

[3]. Sampigethaya, K.,Li, M., Huang, L., Li, M., Poovendran, R., : Amoeba:Robust location privacy scheme for vanet. IEEE Journal on Selected Areas in Communications 25(8), 1569-1589 (2007)

[4]. Yu, Shuyao, Youkun Zhang, Chuck Song, and Kai Chen. "A security architecture for Mobile Ad Hoc Networks", Internet-Draft, April 2003. http://blrc.edu.cn/blrcweb/publication/kc2.pdf

[5]. Milgram, S., "The small world problem," PsychologyToday 1, 61, 1967.

[6]. Razak, S. A., "Two-Tier Intrusion Detection System for Mobile Ad Hoc Network," Ph.D. Thesis, School of Computing, Communications & Electronics, University of Plymouth, 2007.

[7] D. Watts, S.

, "Collective dynamics of 'smallworld' networks". Nature 393 (6684): pp. 440-442, 1998, doi:10.1038/30918.

[8] J. M. Kleinberg, "Navigation in the small world", Nature 406, p. 845, 2000, doi:10.1038/35022643.

[9]. Y. Xia, G. Song, and Y. Zheng, "SW-R2P: A Trusted Small World Overlay P2P Network with Zero Knowledge Identification", Journal of Computers, 3(10):3-11, 2008, doi:10.4304/jcp.3.10.3-11.

[10]. P. Guangyu, M. Gerla, and C. Tsu-Wei, Fisheye state routing: a routing scheme for ad hoc wireless networks. In Proc. IEEE International Conference on Communications (ICC'2000), Vol. 1, pp. 70–74, Vol. b1, Orleans, LA, 18–22 June 2000.

[11]. C. E. Perkins and E. M. Royer, Ad-hoc on-demand distance vector routing. In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), pp. 90–100, New Orleans, LA, 25–26 Feb. 1999.

[12]. D. B. Johnson, D. A. Maltz, and Y.-C. Hu, The dynamic source routing for mobile ad hoc networks. Internet-Draft, draft-ietfmanet-dsr-10.txt, work-in-progress, 2004.

[13]. H. Xiaoyan, X. Kaixin and M. Gerla, Scalable routing protocols for mobile ad hoc networks, IEEE Network, Vol. 16, pp. 11–21, 2002.

[14]. J. Y. Yu and P. H. J. Chong, A survey of clustering schemes for mobile ad hoc networks, IEEE Communications Surveys & Tutorials, Vol. 7, pp. 32–48, 2005.

[15] Mingliang, J., Y. C. Tay, et al. (1999). CBRP: a cluster based routing protocol for mobile ad hoc networks.

[16] C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel" Proc. IEEE SICON'97, Apr.1997, pp.197-211.