International Journal of Smart Sensor and Adhoc Network

Volume 2 | Issue 2 Article 4

January 2012

EFFICIENT AND SECURE AUTHENTICATION BY USING 3-PATH TRANSMISSION IN AD HOC NETWORKS

VETRI SELVI . S
Dept of Computer Science and Engineering, GKM College of Engineering and Technology, Chennai, India.,
vetriselvi.sanj@gmail.com

PURUS HOTHAMAN
Dept of Computer Science and Engineering ,GKM College of Engineering and Technology, Chennai, India,
purush82@gmail.com

EFFICIENT AND SECURE AUTHENTICATION BY USING 3-PATH TRANSMISSION IN AD HOC NETWORKS

VETRI SELVI .S[1], PURUSHOTHAMAN[2]

[1]Assistant Professor, Dept of Computer Science and Engineering, GKM College of Engineering and Technology, Chennai, India.
[2]Dept of Computer Science and Engineering ,GKM College of Engineering and Technology, Chennai, India.
Email: vetriselvi.sanj@gmail.com, purush82@gmail.com

Abstract-Ad hoc networks are created dynamically and maintained by the individual nodes comprising the network. They do not require a pre-existing architecture for communication purposes and do not rely on any form of wired infrastructure; in an ad hoc network all communication occurs through a wireless median. The design and management of ad-hoc networks is significantly a challenging one when compared to contemporary networks. Authenticating the multicast session is an important one. To authenticate several factors should be considered, major issue are resource constraints and the wireless links. In addition to being resource efficient and robust, security solution must be provides to large group of receivers and to long multi-hop paths. The authentication must be done without much delay and should independent of the other packets. In existing TAM Tired Authentication scheme for Multicast traffic is proposed for ad-hoc networks. It exposed network clustering to reduce the overhead and to improve the scalability. Its two tired hierarchy combines the time and secret-information asymmetry to achieve the resource efficiency and scalability. In the proposed system, a Asynchronous authentication scheme as using shared key management is proposed to resolve the foremost conflicting security requirements like group authentication and conditional privacy. The proposed batch verification scheme as a part of the protocol poses a significant reduction within the message delay, then by using shared key process so requirement of the storage management is extremely less.

Keywords*: Ad hoc Network, Clustering, Performance, Security.*

I. INTRODUCTION

Wireless and mobile networks represent an increasingly important segment of networking research as a whole, driven by the rapid growth of portable computing, communication and embedded devices connected to the Internet. Overall, it is clear that mobile, wireless and sensor devices will definitely outnumber wired end-user terminals on the Internet in the near future, strongly motivating consideration of fundamentally new network architectures and services to meet dynamic needs. Over successive 10-15 years, it is anticipated that important qualitative changes to the Internet will be driven by the fast proliferation of mobile
and wireless devices, which may be expected to outnumber wired PC's as early as 2010. The potential impact of the future wireless Internet is extremely important because the network combines the power of computation, search engines and databases in the background with the immediacy of knowledge from mobile users and sensors within the foreground. Wireless networks are of a basically different character: To begin with, wireless connections are by nature significantly fewer stable than wired connections.

Effects influencing propagation of the radio signals, such as reflection, shielding, scattering, and interference, inevitably need routing systems in ad hoc networks to be able to cope with relatively low link communication reliability. Also, several scenarios for ad hoc networks assume that nodes are potentially mobile.

Sources of Challenges in Wireless Networks Features of the Wireless Medium

There are several features of the wireless medium that distinguish it from other media. The wireless medium is a *shared* medium. This means that unlike wire line systems, where there exist dedicated physical connections between users, every user can essentially receive an attenuated version what alternate users are transmitting. In such a system, the manner of transmission is *broadcast* of the signal and there's interference in reception of a signal. Another property of a wireless channel is its random time- varying behavior due to the mobility of users and other objects, as well as obstacles within the
environment.

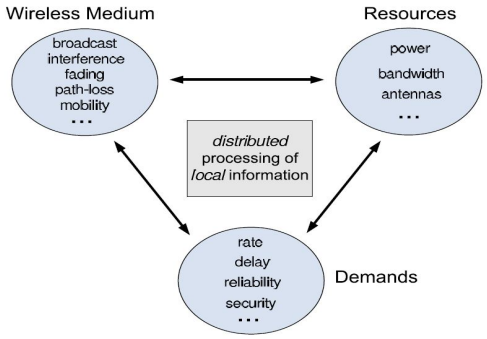

Fig: Sources of challenges in analysis and design of wireless networks.

More specifically, the channel to a given user might have poor conditions at some times and favorable conditions at other times. This is called the *fading* behavior of the channel. In several situations, multiple copies of the transmitted signal could also be received with different delays and strengths. This is often referred to as "multipath fading" and can severely deteriorate the performance once the transmitted signals have shorter duration (e.g., broadband transmission). Conventionally, the goal is to combat randomness introduced by the environment. Though, in recent years, there has been another view and that is to use the inherent randomness in the environment to extend the performance.

For instance, the multi-user diversity gain in the downlink of cellular systems is based on this concept, i.e., in a system of the many users with random quality of reception (fading), there exists one user with high quality of reception with terribly high probability.

Efficient Use of Resources

Today's wireless systems are faced with associate ever-growing demand for higher rates and quality of services. However, the available resources such as bandwidth, power, and variety of antennas are limited. Therefore, efficient usage and allocation of these resources is more important than ever. In several scenarios, from mobile users in cellular networks to sensor nodes deployed in a remote area, the components of the network have limited power supplies. In these networks, efficient use of the available energy (power) supply is a critical issue. Bandwidth is another valuable resource in wireless systems, especially in high data rate broadband communications. Also, there has been an excellent interest in exploiting the spatial degrees of freedom in wireless systems by deploying many antennas at the transmitter and the receiver. The possibility of using multiple antennas in a network (multi-user) setup has been recently explored.

Demands and Services

As mentioned earlier, wireless systems have become highly heterogeneous. Different types of applications like internet, voice, and video-on-demand, are provided over wireless networks. Depending on the application, the main performance measure will vary. For example, video-on-demand applications not only need high rates however are sensitive to delay. For several detection schemes, in ad-hoc networks reliability is that the main concern. In several scenarios, resource allocation in wireless networks aims at optimizing over two conflicting performance measures at the equivalent time, such as reliability and rate or delay and rate. Finding strategies that provide these different demands in an efficient manner could be a difficult task.

Security and Multicasting: a Complex Deal

The IP multicast model is attractive since it can scale to a large number of members. However, scalability is achieved due to the fact that no host identification data is maintained by the routers. Any host in a subnet will be a part of multicast group without its subnet router passing identification data regarding the host to other routers in distribution tree. This simplicity which makes the strength of multicast routing, presents however, many vulnerabilities:

1. IP multicast does not support closed groups. In fact, multicast addresses are publicly known: joining or leaving a group does not require specific permissions. Hence, any user can join a multicast group and receive messages sent to the group.
2. There is no access control to a multicast group: an intruder can send data to the group without being a valid member, and disturbs the multicast session or eventually create bottlenecks in the network (Denial of Service attack).
3. Data sent to the group may transit via many unsecure channels. Thus, eavesdropping opportunities are more important.

Security threats and countermeasures

There exist several security threats, inherent to the distributed and open nature of IP multicast, that require security countermeasures (cf. figure 1).

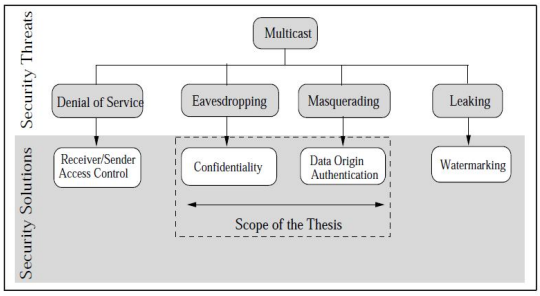

Fig1.Multicast Security Threats and their Countermeasures

Denial of Service / Access Control: in the basic IP multicast model, any node can send data to a multicast session, and any node can become a member of any multicast session. It is clear that this model is vulnerable to Denial of Service (DoS) attacks, where fraudulent users join or send data to multicast sessions only to waste bandwidth or to overwhelm other group members with garbage data or malicious code. Solving these problems requires controlling the ability of hosts to send data or to affix a multicast tree distribution. These are called respectively: sender and receiver access control.

Eavesdropping / Confidentiality: in unicast communication, two users can provide confidentiality by encrypting data with a shared key. In multicast communication, a group key is given to every authorized member. This group key is used by the sender as a symmetric key to encipher the multicast traffic. This becomes complicated when group

membership is dynamic (members join and leave continuously the multicast session). Research work in group key management aims to provide efficient re-keying schemes for dynamic membership groups.

Masquerading / Data Origin Authentication: data origin authentication is the ability of group members to verify the identity of the sender of a received packet. There has been work that aims to efficiently provide this level of authentication.

Leaking / Watermarking: encryption is generally used to safeguard content while it is being transmitted so that unauthorized persons cannot read the stream from the network, but this offers no protection after the intended receiver receives the data. There is no protection against unauthorized duplication and propagation by the intended receiver. Watermarking can provide protection in the form of theft deterrence. Watermarking is the embedding of some identifying information into the content in such a way that it cannot be removed by the user but can be extracted or read by the appropriate party.

II. RELATED WORKS

In this section, we illustrate few methods used so far for the source authentication & clustering methods. In Previous researches, Tired Authentication method was being used for authenticating Source & for Message Integrity. Source Authentication schemes used for multicast traffic in wired and single-hop wireless networks unsuitable for ad-hoc networks. TAM exploits network clustering in order to cut overhead and ensure scalability. It achieves Intra-cluster Source Authentication and Inter-Cluster Authentication. [8] The same kind of Research had been done before to TAM in the name of TESLA. [8] But the Main difference between TESLA & TAM was Time Asymmetry & Secret Information Asymmetry. [8]
Adrian Perrig & Ran Canetti had undergone a research in terms of TESLA, They had given the results: The main challenges of securing multicast communication is source authentication, or enabling receivers of multicast information to verify that the received data originated with the claimed source and was not modified enroute. [10]

The main idea of TESLA; is to have the sender attach to each packet a MAC computed using a key known only to itself. The receiver buffers the received packet while not having the ability to authenticate it. If the packet is received too late, it is discarded. [10] But Even though the TESLA was very suitable for Source Authentication & Message Integrity but there was a limitation in TESLA protocol is that the receiver needs to buffer packets during one disclosure delay before it can authenticate them.

In 2011, Yunhao Liu & Jinsong Han proposed that, Anonymizing Peer-to-Peer (P2P) systems often incurs extra traffic costs , many systems try to mask the identities of their users for privacy considerations.[9] Existing anonymity approaches are mainly path-based: peers have to pre-construct an anonymous path before transmission. The overhead of maintaining and updating such ways is significantly high and propose Rumor Riding (RR), a lightweight and non-path-based mutual anonymity protocol for decentralized P2P systems. Employing a random walk mechanism, RR takes advantage of lower overhead by mainly using the symmetric cryptographic algorithm.[9]

Rumor Riding; select the random walk as the rumor spreading method. Rumor Riding (RR), a lightweight and non-path-based mutual anonymity protocol for decentralized P2P systems.[9] A Non-path-based anonymous P2P protocol called Rumor Riding (RR).

To address security issues in the heterogeneous WSNs, propose a secure clustering scheme along with a deterministic pairwise key management scheme based on public key cryptography [11]. The proposed security mechanism guarantees that any two sensor nodes located in the same cluster and routing path can directly establish a pairwise key without disclosing any information to other nodes. To Achieve security Problems in Ad hoc Networks , Reza Azarderskhsh and Arash Reyhani-Masoleh gave their research results are Information security in infrastructureless wireless sensor networks (WSNs) a secure clustering scheme along with a deterministic pairwise key management scheme based on public key cryptography to be mainly focused.[11]
Scientists Shuhui Yang, Jie Wu, Jiannong Cao found that A connected k-hop clustering network is formed by electing cluster-heads in k-hop neighborhoods and finding gateway nodes to connect cluster-heads. In their paper, the adjacency-based neighbor cluster-head selection rule (A-NCR) by extend the “2.5” hops coverage theorem and generalizing it to k-hop cluster.[12] The results show that the proposed approaches generate a connected k-hop clustering network, and reduce the number of gateway nodes effectively. They gave their results that If the energy has to saved and signal collision has to be reduced, the number of these gateway nodes should be as few as possible. Clustering protocols should be oriented towards power-saving and energy-efficiency.

Dewan Tanvir Ahmed from University of Ottawa said that Multicasting is intended for group communication that supports the dissemination of information from a sender to all the receivers in a group [14].Two well-known examples of tree-based multicast routing protocols are the Multicast Ad hoc On-demand Distance Vector routing protocol

(MAODV), and the Adaptive Demand-driven Multicast Routing protocol (ADMR).

In 2006, one of the main challenges is to judge whether or not a routing message originates from a trustworthy node. The answer to this point is cryptographically signed messages. The common assumption is that nodes in possession of a valid secret key can be trusted. Consequently, a secure and efficient key-management scheme is crucial. Keys also are needed for protection of application data. [15] Keys are a prerequisite to bootstrap a protected network service. This article surveys the state of the art within key management for ad hoc networks, and analyzes their applicability for network-layer security. The solution would provide little flexibility and scale badly.

Ossama Younis and Sonia Fahmy, Research Scholars from Purdue University researched in topic - a new energy - efficient approach for clustering nodes in ad hoc sensor networks.[16] Based on this approach, a protocol, HEED (Hybrid Energy-Efficient Distributed clustering), that periodically chooses the cluster heads according to a hybrid of their residual energy and a secondary parameter, such as node proximity to its neighbors or node degree.

For Multicast stream Authentication Purpose, Adrian Perrig, Ran Canetti, IBM T.J. Watson proposed two schemes TESLA & EMSS. [3] TESLA has been discussed before, as it offers sender authentication, high scalability, strong loss robustness, and minimal overhead, at the cost of loose initial time synchronization and slightly delayed authentication and for EMSS, It offers non repudiation of origin, more loss resistance, and less overhead, at the cost of slightly delayed verification.

Dirk Balfanz, D. K. Smetters proposed a solution for secure communication and authentication in ad-hoc wireless networks & also for presented new schemes for peer-to-peer authentication in ad-hoc wireless networks.[6] Some of the Important Schemes which has been introduced by them are Use of location-limited channels, Novel location-limited channels, Concrete pre-authentication protocols, Group communication, No reliance on Public Key Infrastructure.

In 2002, A Research has been proposed a System for one-time signature scheme called “BiBa”(for “Bins and Balls”).[7] But BiBa’s main disadvantage is the time required to sign a message, which is longer than in most previously proposed one-time signature schemes.

Moustafa A. Youssef & his team proposed a randomized, distributed multihop clustering algorithm (KOCA) for solving the overlapping clustering problem.[5] KOCA aims at generating connected overlapping clusters that cover the entire sensor network with a specific average overlapping degree. Although KOCA generates overlapping clusters, the simulation results show that the clusters are approximately same in size. This is desirable to achieve load balancing between different clusters.

III. SYSTEM MODEL:

Architecture Model

The simulation work has been done with The Network Simulator ns-2, Version 2.29. In the simulation 50 nodes are randomly distributed within the network field of size 2400mx2400m. Ad hoc network topology is formed with the help of various nodes creation. Clusters are formed based on the location and their connectivity with other nodes. Each cluster is controlled by the cluster heads from them only messages are passed to another cluster. Source nodes are in connection with cluster heads.

Key Establishment

In our proposed we use RSA based key generation. And then we use of hashing technique for memory optimization. One pair wise key and one shared key will be created.

Group key management (intra cluster)

Nodes get keys dynamically in the key distribution phase and then start to broadcast their geographic based. All nodes getting keys from the same leaderform a group, as illustrated in the communication range of RSUs is 300 meter. The key was asymmetric based group key method in both Leader and member have a common key for sharing.

Shared key management (inter cluster)

Leader get keys dynamically in the key distribution phase and then start to broadcast their geographic condition messages per. All leader nodes getting keys from the server form, as illustrated in the communication range of leader is 300 meter. The key was asymmetric based shared key method in each cluster heads have a common key for sharing.

Path selection

The path selection is a very important problem in the context of Ant Colony Optimization because it is the problem to which the original AS was first applied, and it has later often been used as a benchmark to test a new idea and algorithmic variants. In the transmission of data packet in the network, the encrypted data, hash key and public key are transmitting in the three different paths for the further more security. [18]

Positive Feedback accounts for rapid discovery of good solutions. Distributed computation avoids premature convergence. The greedy heuristic helps find acceptable solution in the early solution in the early stages of the search process. The collective interaction of a population of agents.

Performance Evaluation

Performance can be compared by analyzing both the theoretical and simulation results under our protocol with those under the protocol in since the cooperative authentication protocol is of particularly importance in the high-load scenario, we thus only focus on the highway scenario in this part. The best case and worst case performance is analyzed.

IV. CONCLUSION

This paper has presented efficient and secure authentication of the source and to prevent the messages from intruders. It proposed two tired for time and secret data asymmetry in order to achieve the scalability and resource efficiency. The performance has been analyzed mathematically and through simulation. The future work plan includes studying the efficiency of cluster on the performance of three path transmission.

REFERENCES

[1] F. Richard Yu, Helen Tang, Peter C. Mason, and Fei Wang, "A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks", IEEE Transactions on Network and Service Management, Vol. 7, No. 4, December 2010.

[2] Leonid Reyzin, and Natan Reyzin, "Better than BiBa short one-time signatures with fast signing and verifying", October 17, 2007.

[3] Adrian Perrig, Ran Canetti, J. D. Tygar, Dawn Song, IBM T.J. Watson and UC Berkeley, "Efficient Authentication and Signing ofmulticast streams lossy channels", perrig,tygar,dawnsong@cs.berkeley.edu, canetti@watson.ibm.com.

[4] M.F. Younis, K. Ghumman, M. Eltoweiisy, "Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 17, Aug. 2006, pp. 865-882.

[5] Moustafa A. Youssef, Adel Youssef, Mohamed F. Younis, "Overlapping Multihop Clustering for Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 20, NO. 12, December 2009.

[6] Dirk Balfanz, D. K. Smetters, Paul Stewart and H. Chi Wong ,"Talking To Strangers Authentication in AdHoc Wireless Networks", balfanz,smetters,stewart,hcwong@parc.xerox.com

[7] Adrian Perrig, "The BiBa one-time signature and broadcast authentication", University of California, Berkeley, perrig@cs.berkeley.edu

[8] Mohamed Younis and Osama Farrag, "TAM: A Tiered Authentication of Multicast Protocol for Ad-Hoc Networks" at IEEE Transactions on Network and Service Management Vol. 9, No. 1, pages 100-113, March 2012.

[9] Yunhao Liu, Jinsong Han, and Jilong Wang, "Rumor Riding: Anonymizing Unstructured Peer-to-Peer Systems" at IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 3, pages 464-475, March 2011.

[10] Adrian Perrig, Ran Canetti, Dawn Song, J. D. Tygar, "Efficient and Secure Source Authentication for Multicast" perrig,dawnsong,tygar@cs.berkeley.edu, canetti@watson.ibm.com.

[11] Reza Azarderskhsh and Arash Reyhani-Masoleh, "Secure Clustering and Symmetric Key Establishment in Heterogeneous WSNs", Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking Volume 2011, Article ID 893592, pages 1-12, October 2010.

[12] Shuhui Yang, Jie Wu, Jiannong Cao, "Connected k-Hop Clustering in AdHoc Networks", sjcao@comp.polyu.edu. hk syang1@fau.edu,jie@cse.fau.edu

[13] Edith C.H. Ngai and Michael R. Lyu "An Authentication Service Based on Trust and Clustering in WSNs", Department of Computer Science and Engineering, The Chinese University of Hong Kong{chngai, lyu}@cse.cuhk.edu.hk

[14] Dewan Tanvir Ahmed, " Multicasting in Ad Hoc Networks" University of Ottawa dahmed@site.uottawa.ca, 2005.

[15] Anne Marie Hegland, Eliwinjum, Stig F. Mjolsnes, Chunming Rong, Oivind Kure, and Pal Spilling," A Survey of Key Management in Ad Hoc Networks" Attacker" IEEE Communications surveys, The Electronic of Original Peer-Reviewed Survey Articles, www.comsoc.org/pubs/surveys, Vol.8,No.3, pages 48-66,3rd Quarter2006.

[16] Ossama Younis and Sonia Fahmy, "Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach", Department of Computer Sciences, Purdue University, pages 1-12.

[17] Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks", Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648/02 $17.00 © 2002

[18] http://www.idsia.ch/~gianni/AntHocNet/anthocnet.html, "The anthocnet routing algorithm for manets".