RESEARCH PAPER | Computer Science | Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

Providing the Source Authentication and Efficient Mulicast Communication in Wireless Adhoc Networks

KEYWORDS: Multicast communication traffic, message authentication, ad-hoc networks

G. Prabaharan
Assistant professor/CSE, Adhiparasakthi Engineering College, Melmaruvathur.

P. Nandhini
ME Computerscience and Engineering, Adhiparasakthi Engineering College, Melmaruvathur.

ABSTRACT *Ad-hoc networks are becoming an effective tool for many mission critical applications such as troop coordination in a combat field and situational awareness, etc. for that it need multicast style of communication traffic. Ad-hoc Networks applications are characterized by the hostile environment that they serve in and by the multicast-style of communication traffic. Authenticating the source and ensuring the integrity of the message traffic become a fundamental requirement for the operation and management of the network. Efficient and secure source Authentication scheme for Multicast traffic is used for large scale dense ad-hoc networks and the source authentication scheme for secret information asymmetry, hybrid asymmetry and time asymmetry. The receiver can verify the message origin using the MAC. This property is used for providing data sources for preventing impersonation.*

1. INTRODUCTION

Ad-hoc network is a decentralized type of wireless network. The adhoc network does not depend on routers in wired networks or access points in a wireless networks. In recent years ad-hoc networks have been attracting increased attention from the engineering community and research motivated by applications like asset tracking, digital battlefield, air-borne safety, border protection and situational awareness. The efficient network management solutions suitable for nodes that are constrained in on-board energy and in their computation and communication capacities, it is important to devise for these network applications.

In addition, to rely on multicast for management-related control traffic such as neighbour/route discovery to setup the establishment of time synchronization, multihop paths etc., is common for ad-hoc networks. Such multicast traffic among the nodes in the adhoc network has to be delivered in a secure and trusted manner. Providing an efficient multicast message and source authentication security service that can easily scale for large networks is an important capability for the operation and management of the underlying network.

In existing system Group communication is considered a critical service in adhoc networks due to their inherently contributive operations, where the nodes cooperate in network management and strive to accomplish common missions autonomously in highly unpredictable environment without reliance on infrastructure. The limited computational, the large scale deployment and the unguaranteed connectivity to trusted authorities make known solutions for wired and single-hop wireless networks.

II. PROPOSED SYSTEM

The secure source authentication for multicast in adhoc networks is used to develop a Tiered Authentication scheme for Multicast traffic for large scale dense ad-hoc networks. It combines the advantages of the time asymmetry and the secret information asymmetry paradigms and exploits network clustering to reduce overhead and ensure scalability. Multicast traffic within a cluster employs a one-way hash function chain in order to authenticate the message source. Cross-cluster multicast traffic includes message authentication codes (MACs) that are based on a set of keys. Each cluster uses a unique subset of keys to look for its distinct combination of valid MACs in the message in order to authenticate the source. The asymmetry property denotes that a receiver can verify the message origin using the MAC in a packet without knowing how to generate the MAC. This property is the key for preventing impersonation of data sources.

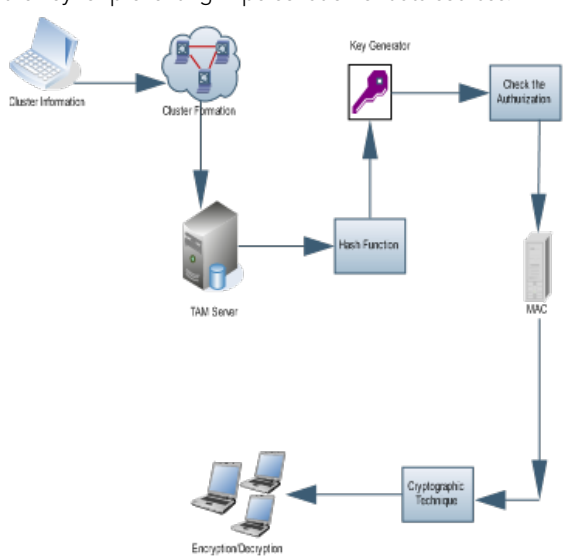

Fig. 1.System Architecture

Depending on the applications, an ad-hoc network may include up to a few hundreds or even a thousand nodes. Communications among nodes are via multihop routes using omnidirectional wireless broadcasts with limited transmission range. In the system model considered in this paper, nodes are grouped into clusters. The clusters formation can be based on location and radio connectivity. It is assumed that clusters are established securely by using pre-distributed public keys, employing a robust trust model or applying identity based asymmetric key-pair cryptographic methods and that a proper key management protocol is followed in order to perform clustering when needed. Clustering is a popular architectural mechanism for enabling scalability of network management functions. It has been shown that clustered network topologies better support routing of multicast traffic and the performance gain dominates the overhead of creating and maintaining the clusters.

III. MODULES WITH DESCRIPTION

A. Deployment of cluster formation

In the cluster formation, to create the Users enter the Node Name, IpAddress, port number, Group Name of the node to register in the Database. While entering the next node the

Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

user must check the database for that node exists or new one. If the node is already available the server informs to the user, otherwise the new cluster is created.

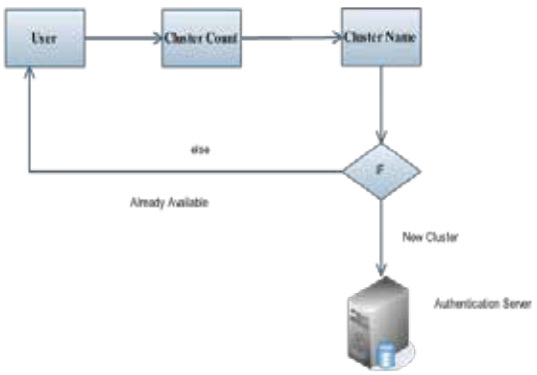

Fig. 2 Block diagram for Deployment of cluster formation

B. Authenticate the source and message

A security solution should scale for large group of receivers and long multi-hop paths. Thus, a solution that is based on a distinct authentication key for every receiver will introduce prohibitive overhead to the message and consume significant portion of the available bandwidth. Moreover, the solution should scale for large number of senders by requiring reasonable memory resources at the individual receivers for storing authentication keys. Finally, it is desired to enable the validation of every packet without excessive delay and independent of the other packets.

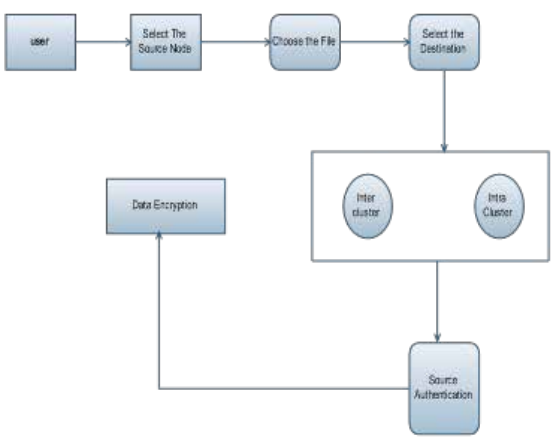

Fig. 3 Block diagram for Authenticate The Source And Message

C. MAC generation and Dissimination

Cross-cluster multicast traffic includes message authentication codes (MACs) that are based on multiple keys. Each cluster looks for a distinct combination of MACs in the message in order to authenticate the source. The source generates the keys at the time of establishing the multicast session. The keys will be securely transmitted to the head of every cluster that hosts one or multiple receivers. The multicast message is then transmitted to the cluster-heads which authenticate the source and then deliver the message to the intended receivers using the intra-cluster authentication scheme. The rationale is that the MAC will be associated with the cluster rather than the nodes and thus the overhead is reduced significantly.

D. Authorization for cluster node

After generation of MAC by the source, It can be broadcast the message to particular destination whether the destination may be internal cluster or not. If the node is in valid state Perform some action.

IV. RELATED WORK

Authenticated signature Algorithm and Message Authentication code is used for multicast traffic in adhoc networks

A. AUTHENTICATED SIGNATURE ALGORITHM

Authenticated Signature Algorithm use public key algorithms to provide data integrity. When you sign data with a digital signature, someone else can verify the signature, and can prove that the data originated from you and was not altered after you signed it.

Authenticated signature scheme given prime p, public random number g, private (key) random number x, compute

$y = g^x \pmod p$

public key is (y,g,p)

nb (g,p) may be shared by many users

p must be large enough so discrete log is hard

private key is (x)

to sign a message M

choose a random number k, GCD(k,p-1)=1

compute

$a = g^k \pmod p$

use extended Euclidean (inverse) algorithm to solve

$M = x.a + k.b \pmod{p-1}$

the signature is (a,b), k must be kept secret

to verify a signature (a,b) confirm:

$y^a.a^b \pmod p = g^M \pmod p$

B. MESSAGE AUTHENTICATION CODE

consistent initialize( )

while consistent do

(X; valx) select(V ar, 0)

if solve((X; valx), V ar n fXg, Sol, 1) then

return true

DxDx n fvalx g

consistentDx =6 ; and propagate(V ar n fXg, 1)

solve(in: (X; valx), V ar, Sol, level ; out: Sol) return boolean

Sol Sol[f(X; valx)g

if level = N then

return true

for each a 2 Dx, a =6 valx do

DxDx n fag

consistent propagate(V ar, level)

Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

while consistent do

(Y; valy) select(V ar, level)

if solve((Y; valy), V ar n fY g, Sol, level+1)

return true

DyDy n fvalyg

consistentDy =6 ; and propagate(V ar n fY g, level)

Sol Sol n f(X; valx)g

restore(level)

return false

B. CONCLUSION

The collaborative nature of these applications makes multicast traffic very common. Securing such traffic is of great importance, particularly authenticating the source and message to prevent any infiltration attempts by an intruder. Contemporary source authentication schemes found in the literature either introduce excessive overhead or do not scale for large networks. The efficient and secure source authentication of multicast traffic, which pursues a two tired hierarchical strategy combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency. The performance has been analysed mathematically and through simulation, confirming its effectiveness. In addition, the effect of the various parameters has been studied and guidelines have been highlighted for picking the most suitable configuration in the context of the particular application requirements.

REFERENCE [1] J. Y. Yu and P. H. J. Chong, "A survey of clustering schemes for mobile ad hoc networks," IEEE Commun. Surveys & Tutorials, vol. 1, no. 1,pp. 31–48, 2005. | [2] P. B. Velloso, et al., "Trust management in mobile ad hoc networks using a scalable maturity-based model," IEEE Trans. Network Service Management, vol. 7, no. 3, Sep. 2010. | [3]G. Angione, P. Bellavista, A. Corradi, and E. Magistretti, "A k-hop clustering protocol for dense mobile ad-hoc networks," in Proc. 2006IEEE International Conf. Distrib. Computing Systems Workshop. | [4] E. M. Royer and C. Perkins, "Multicast ad-hoc on-demand distance vector (MAODV) routing," Internet Draft, University of California, Charles E. Perkins Nokia Research Centre, July 2000. | [5]Y. Zhu and T. Kunz, "MAODV implementation for NS-2.26," Technical Report SCE-04-01, Dept. of Systems and Computing Engineering, Carleton University, Jan. 2004. | [6] M. Youssef, A. Youssef, and M. Younis, "Overlapping multihop clustering for wireless sensor networks," IEEE Trans. Parallel Distrib. Syst.,vol. 20no. 12, pp. 1844–1856, Dec. 2009. | [7] J. Y. Yu and P. H. J. Chong, "A survey of clustering schemes for mobile ad hoc networks," IEEE Commun. Surveys & Tutorials, vol. 1, no. 1,pp. 31–48, 2005. | [8] P. B. Velloso, et al., "Trust management in mobile ad hoc networks using a scalable maturity-based model," IEEE Trans. Network Service Management, vol. 7, no. 3, Sep. 2010. | [9]C. R. Lin and M. Gerla, " A Distributed Control Scheme in Multi-hop Packet Radio Networks for Voice/Data Traffic Support," Proc. IEEE ICC'95, June 1995, pp. 1238–42. | [10] U. C. Kozat et al., "Virtual Dynamic Backbone for Mobile AdHoc Networks," Proc. IEEE ICC'01, vol. 1, June 2001, pp.250–55. | [11] M. R. Pearlman and Z. J. Haas, "Determining the Optimal Configuration for the Zone Routing Protocol," IEEE JSAC, vol. 17, Aug. 1999, pp. 1395–414. | [12] A. Iwata et al., "Scalable Routing Strategies for Ad Hoc Wireless Networks," IEEE JSAC, vol. 17, Aug. 1999, pp. 1369–79