International Journal of Current Engineering and Technology
ISSN 2277 – 4106
©2013 INPRESSCO. All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

TAM: Tiered Authentication Of Multicast Protocol For Adhoc network

Lasya.R[a*] and B.A.Patil[b]

[a]Department of CSE, Visvesvaraya Technological University, Belgaum, Karnataka
[b]Department of computer science and engineering, KLE college of engineering, Belgaum, Karnataka

Abstract

Ad-hoc networks are becoming an effective tool for many mission critical applications such as troop coordination in a combat field, situational awareness, etc. These applications are characterized by the hostile environment that they serve in and by the multicast-style of communication traffic. Therefore, authenticating the source and ensuring the integrity of the message traffic become a fundamental requirement for the operation and management of the network. However, the limited computation and communication resources, the large scale deployment and the unguaranteed connectivity to trusted authorities make known solutions for wired and single-hop wireless networks inappropriate. This paper presents a new Tiered Authentication scheme for Multicast traffic (TAM) for large scale dense ad-hoc networks. TAM 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 simulation and analytical results demonstrate the performance advantage of TAM in terms of bandwidth overhead and delivery delay.

Keywords: *Multicast communications, message authentication, ad-hoc networks.*

1. Introduction

The continual advancement in wireless technologies has enabled networked-solutions for many nonconventional civil and military applications. In recent years ad-hoc networks have been attracting increased attention from the research and engineering community, motivated by applications like digital battlefield, asset tracking, air-borne safety, situational awareness, and border protection . In these network applications, it is important to devise efficient network management solutions suitable for nodes that are constrained in onboard energy and in their computation and communication capacities.

In addition, the solutions must be scalable to support networks covering vast areas with a large set of nodes that communicate over many hops. These characteristics make the design and management of ad-hoc networks significantly challenging in comparison to contemporary networks. In addition, the great flexibility of ad-hoc networking comes at the price of a increased vulnerability to security attacks and trade-off would be unavoidable at the level of network management and services .

Group communication is considered a critical service in adhoc networks due to their inherently collaborative operations where the nodes cooperate in network management and strive to accomplish common missions autonomously in highly unpredictable environment without reliance on infrastructure equipment. In particular the provided network services need to achieve the following security goals: (1) Confidentiality, to prevent adversaries from reading transmitted data, (2) Message integrity, to prevent tampering with transmitted messages, and (3) Source Authentication, to prevent man-in-the-middle attacks that may replay transmitted data for node impersonation. Confidentiality is achieved by encrypting the transmitted data. The work presented in this paper aims at addressing the second and third goals. 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. Source and message authentication is the corroboration that a message has not been changed and the sender of a message is as claimed to be. This can be done by sending a (1) Cryptographic digital signature, or (2) Message Authentication Code (MAC) . The first involves asymmetric cryptography and often needs heavy computation both at the sender and the receiver.

2. Existing System

*Corresponding author: **Lasya.R**

In recent years ad-hoc networks have been attracting increased attention from the research and engineering community, motivated by applications like digital battlefield, asset tracking, air-borne safety, situational awareness, and border protection. In these network applications, it is important to devise efficient network management solutions suitable for nodes that are constrained in onboard energy and in their computation and communication capacities. In addition, the solutions must be scalable to support networks covering vast areas with a large set of nodes that communicate over many hops. These characteristics make the design and management of ad-hoc networks significantly challenging in comparison to contemporary networks. Group communication is considered a critical service in adhoc networks due to their inherently collaborative operations, where the nodes cooperate in network management and strive to accomplish common missions autonomously in highly unpredictable environment without reliance on infrastructure equipment. The limited computation and communication resources, the large scale deployment and the unguaranteed connectivity to trusted authorities make known solutions for wired and single-hop wireless networks inappropriate.

3. Proposed system

We are going to develop a new Tiered Authentication scheme for Multicast traffic (TAM) for large scale dense ad-hoc networks. TAM 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.

4. Design And Implementation

The system contains two modules:

- Intra-cluster source authentication
- Inter-cluster authentication
- **Intra-cluster source authentication:** Grouping nodes into clusters enables having a reasonably tight bound on the end-to-end delay of packet delivery and will thus enable the use of a time asymmetry based authentication scheme. Intra-cluster authentication in TAM is based on TESLA . Inter-cluster multicast traffic will be authenticating differently as explained below. A source node generates chain of one-time-use keys using the hash function, e.g., MD5 SHA-1, etc., and shares only that last generated key, *Kl*, with the receivers. A message can be authenticated only when the used key in the chain is revealed. Fig demonstrates the authentication process.
- **Inter-cluster authentication:** Authentication based on time asymmetry requires clock synchronization and thus does not suit large networks. For inter-cluster multicast traffic, TAM applies a strategy based on secret information asymmetry and engages the clusterheads in the authentication process.

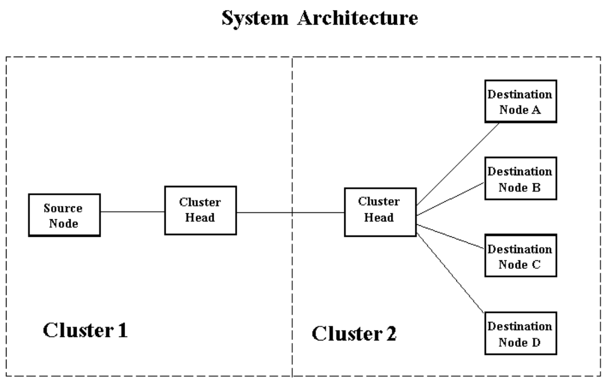


Fig.1 Architecture Diagram

As shown in the figure,

- The cluster 1 contains sourrce node and cluster head and,
- The cluster 2 contains cluster head and destinations.

Message sent from source to destinatons through cluster heads is verified.

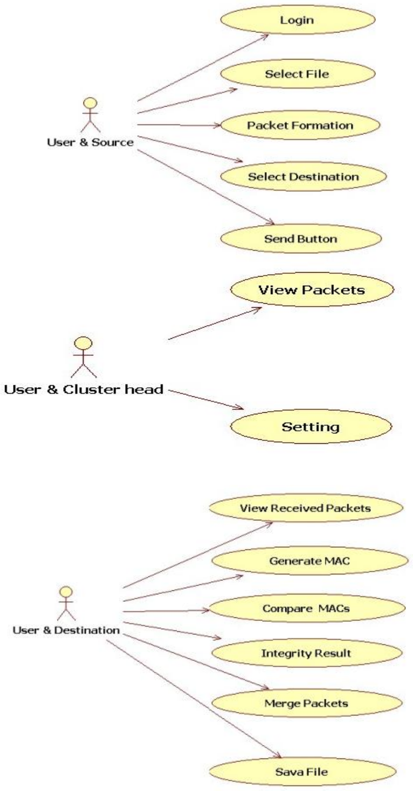


Fig.2 User Case Diagram

5. Module Description

1. **Intra-cluster source authentication:** In this Module, To verify the authentication key, the receiver recursively applies the cryptographic hash function until reaching *Kl*. In reality, the receiver can stop when reaching a key that has been used before. A key cannot be used outside its designated time interval and the message will be ignored if the MAC is based on an expired key. Consequently, clock synchronization is required to make sure that the source and destination have the same time reference for key expiration. Therefore, TAM favors small cluster diameters as will be shown shortly. The approach has two distinct advantages, namely:

• The MAC overhead is small; basically a single MAC is used per every multicast packet for all receivers.

• A missed key in a lost packet would not obstruct the authentication process since a receiver can refer back to *Kl*.

2. **Inter –cluster authentication:** In this module, The multicast group of a source node *s* includes nodes *a*1, *b*1, . . . , *z*1. First, node *s* prepares a MAC corresponding to every cluster targeted by the multicast and appends these MACs to the data packet. The source node then forwards the packet to *CHa*1, *CHb*1, . . . , *CHz*1. Each of the receiving cluster-heads will authenticate the packet using their key share that they got from *s* at the time the multicast session was established. After authenticating the source, each cluster-head forwards the message to the members of the multicast group within its cluster. TAM intra-cluster authentication procedure will be followed inside each cluster, i.e., *CHa*1 will replace the inter-cluster MACs with an intra-cluster timeasymmetry based MAC produced so that receivers like *a*1 can authenticate *CHa*1, and similarly for *CHb*1, . . . , *CHz*1. Fig. 3 summarizes the inter-cluster procedure and implicitly illustrates the intra-cluster authentication process.

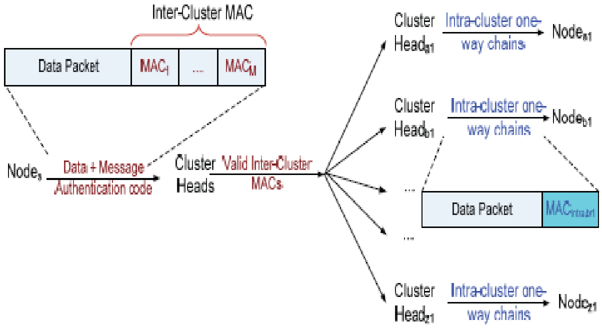
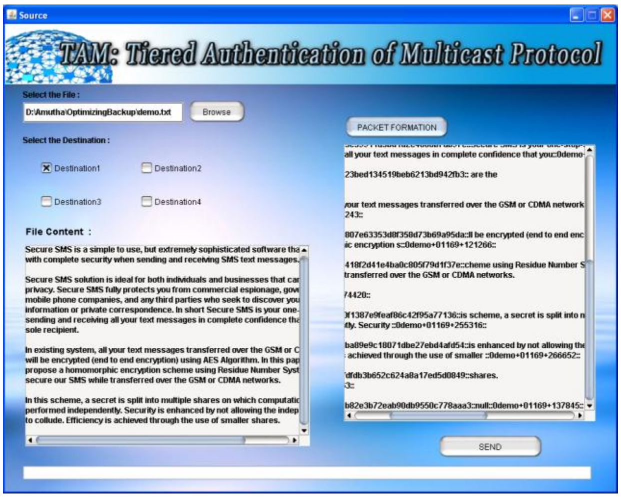


Fig. 3. Illlustrating the steps and packet contents when a node *s* multicast a data packet to nodes *a*1, *b*1,· · · ,*z*1 according to TAM

6. Results



Select the File : D:\Amutha\OptimizingBackup\demo.txt

Select the Destination :

☒ Destination1 ☐ Destination2
☐ Destination3 ☐ Destination4

File Content :

Secure SMS is a simple to use, but extremely sophisticated software tha
with complete security when sending and receiving SMS text messages.

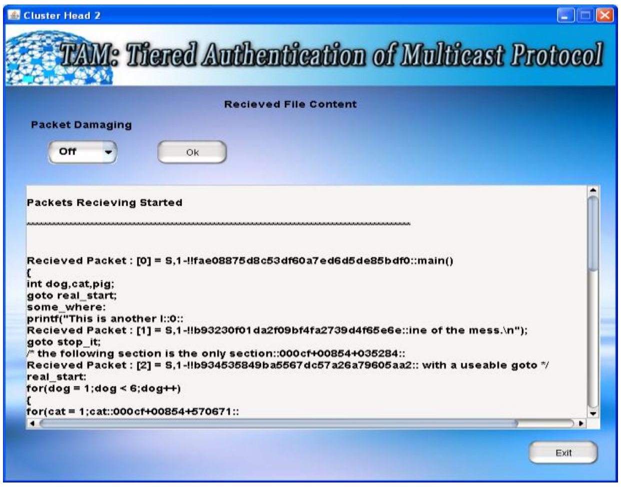
Secure SMS solution is ideal for both individuals and businesses that car
privacy. Secure SMS fully protects you from commercial espionage, gove
mobile phone companies, and any third parties who seek to discover you
information or private correspondence. In short Secure SMS is your one-
sending and receiving all your text messages in complete confidence tha
sole recipient.

In existing system, all your text messages transferred over the GSM or C
will be encrypted (end to end encryption) using AES Algorithm. In this pap
propose a homomorphic encryption scheme using Residue Number Syst
secure our SMS while transferred over the GSM or CDMA networks.

In this scheme, a secret is split into multiple shares on which computatic
performed independently. Security is enhanced by not allowing the indep
to collude. Efficiency is achieved through the use of smaller shares.

```
all your text messages in complete confidence that you::0demo-

23bed134519beb6213bd942fb3:: are the

your text messages transferred over the GSM or CDMA network
243::

807e63353d8f358d73b69a95da::ll be encrypted (end to end enc
ic encryption s::0demo+01169+121266::

418f2d41e4ba0c805f79d1f37e::cheme using Residue Number S
transferred over the GSM or CDMA networks.

74420::

0f1387e9feaf86c42f95a77136::is scheme, a secret is split into n
ntly. Security ::0demo+01169+255316::

ba89e9c18071dbe27ebd4afd54::is enhanced by not allowing the
achieved through the use of smaller ::0demo+01169+266652::

'dfdb3b652c624a8a17ed5d0849::shares.
3::

b82e3b72eab90db9550c778aaa3::null::0demo+01169+137845::
```

Fig.3 Snapshot of source

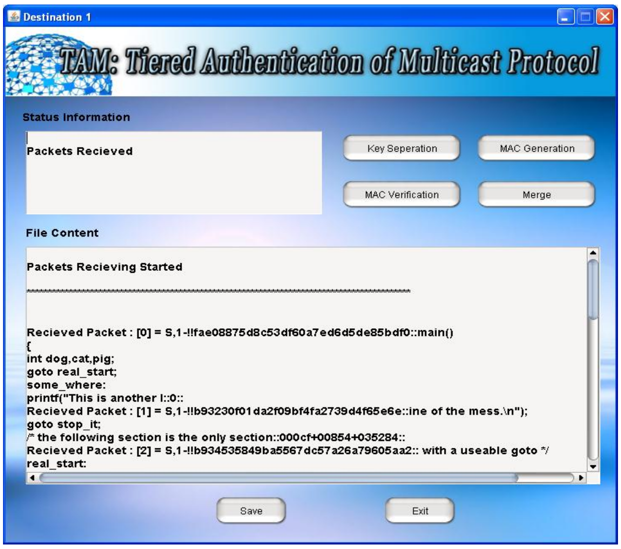


Recieved File Content

Packet Damaging: Off

```
Packets Recieving Started
*****************************************************************************


Recieved Packet : [0] = S,1-!!fae08875d8c53df60a7ed6d5de85bdf0::main()
{
int dog,cat,pig;
goto real_start;
some_where:
printf("This is another l::0::
Recieved Packet : [1] = S,1-!!b93230f01da2f09bf4fa2739d4f65e6e::ine of the mess.\n");
goto stop_it;
/* the following section is the only section::000cf+00854+035284::
Recieved Packet : [2] = S,1-!!b934535849ba5567dc57a26a79605aa2:: with a useable goto */
real_start:
for(dog = 1;dog < 6;dog++)
{
for(cat = 1;cat::000cf+00854+570671::
```

Fig.4 Snapshot of data transferred from source to destination through cluster head



Status Information

Packets Recieved

File Content

```
Packets Recieving Started
*****************************************************************************


Recieved Packet : [0] = S,1-!!fae08875d8c53df60a7ed6d5de85bdf0::main()
{
int dog,cat,pig;
goto real_start;
some_where:
printf("This is another l::0::
Recieved Packet : [1] = S,1-!!b93230f01da2f09bf4fa2739d4f65e6e::ine of the mess.\n");
goto stop_it;
/* the following section is the only section::000cf+00854+035284::
Recieved Packet : [2] = S,1-!!b934535849ba5567dc57a26a79605aa2:: with a useable goto */
real_start:
```

Fig 5. Snapshot of destination , packets received and MAC is verified.

Conclusion

In recent years there has been a growing interest in th use of ad-hoc networks in security-sensitive applications such as digital battlefield, situation awareness, and border protection 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. This paper has presented TAM, which pursues a two tired hierarchical strategy combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency.

The performance of TAM has been analyzed 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; most notably having a cluster radius of 2 or 3 hops appears to be the most suitable for TAM. Our future work plan includes studying the effect of different clustering strategies on the performance of TAM.

References

C. E. Perkins (2001), Ad Hoc Networking. Addison-Wesley.

H. Yang, et al. (2004), Security in mobile ad-hoc wireless networks: challenges and solutions, *IEEE Wireless Commun. Mag*., vol. 11, no. 1, pp. 1536– 1284.

Y. Challal, H. Bettahar, and A. Bouabdallah (2004),, A taxonomy of multicast data origin authentication, issues and solutions, *IEEE Commun. Surveys & Tutorials,* vol. 6, no. 3, pp. 34–57

A. Perrig, R. Canetti, D. Song, and D. Tygar (2000), Efficient authentication and signing of multicast streams over lossy channels, in *Proc. 2000 IEEE Symposium Security Privacy*

R. Canetti et al. (1999), Multicast security: a taxonomy and efficient constructions, in *Proc. 1999 IEEE INFOCOM*

R. Safavi-Naini and H. Wang (May 1999), Multi-receiver authentication codes: models, bounds, constructions, and extensions, *Inf. Computation*, vol. 151, no. 1–2, pp. 148–172.

Perrig, et al. (2001), Efficient and secure source authentication for multicast, *in Proc. 2001 Network Distributed System Security Symposium.*

A. Perrig (2001), The BiBa one-time signature and broadcast authentication protocol, in *Proc. 2001 ACM Conf. Computer Commun. Security*.

L. Reyzin and N. Reyzin (2002), Better than BiBa: short one-time signatures with fast signing and verifying, in *Proc. 2002 Australian Conf. Info. Security Privacy*, pp. 144–153.

A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling (2006), A survey of key management in ad hoc networks, *IEEE Commun. Surveys & Tutorials,* vol. 8, no. 3, pp. 48–66