OPTIMIZED PRIVACY –PRESERVING AUTHENTICATION AND PROTECTION OF NETWORK BY USING DOVE PROTOCOL

[1]ANAND, [2]GUNALAN, [3]VAMSHI, [4]SIDDARTH

[1,2,3,4]Electronics and Communication Engineering, Srm University-Chennai
E-mail: [1]anandmurugan11@gmail.com

Abstract— Networking is currently facing important challenges arising from the advent of virtualization and tunnelling of networks. In this work **,** To disseminate data to a desired number of receivers for efficient privacy preserving authentication using DOVE scheme. To avoid time consuming and to ensure the integrity of messages before batch group authentication by using Hash message authentication code (HMAC) and CMAC (Cipher-based MAC).

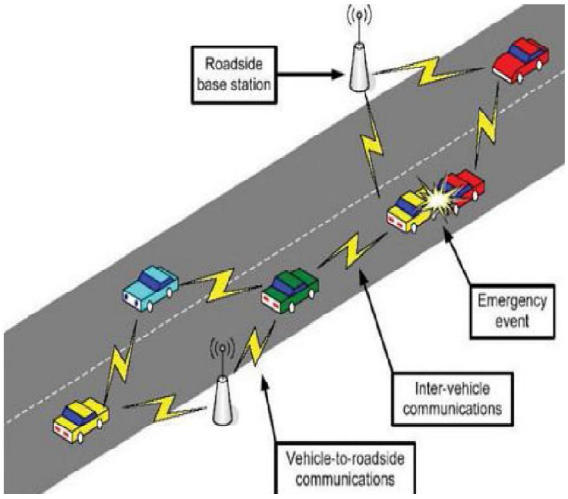
I. INTRODUCTION

- Data dissemination schemes in VANET do not control the number of receivers.
- Extra time for verification and decryption is needed.
- High delay is caused by the CRL checking and group signature verification to achieve the rapid authentication.
- An efficient conditional privacy preserving authentication scheme for VANETs under ISP (Internet Service Provider), by jointly using the techniques of distributed management, HMAC, batch group signature verification, and cooperative authentication.
- First: DOVE reaches the desired number of receivers with little inaccuracy and minimizes the dissemination delay with low communication overhead.
- Second: To calculate HMAC and CMAC (Cipher-based MAC) with the group key generated by the self-healing group-key generation algorithm
- which can replace the time consuming CRL checking and ensure the integrity of messages before batch verification

Vehicular Ad-Hoc Network (VANET):

In VANET is an

- Intelligent Vehicular Ad Hoc Networking for easy and effective communication between vehicles with dynamic mobility.
- VANET, is a form of Mobile ad-hoc network,
- to provide communications among nearby vehicles and
- between vehicles and nearby fixed equipment, usually described as roadside equipment.
- In intelligent vehicular ad hoc network, rather than moving at random as in MANET vehicles tend to move in an organized fashion.
- Providing vehicle-to-vehicle and
- vehicle-to-roadside communication can considerably improve traffic safety and comfort of driving and traveling.



Communication Protocols:

- **User Datagram Protocol (UDP)**
- **Transmission Control Protocol (TCP)**

User Datagram Protocol (UDP)

- UDP uses a simple connectionless transmission model with a minimum of protocol mechanism.
- It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network protocol. There is no guarantee of delivery, ordering, or duplicate protection.
- UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.
- With UDP, computer applications can send messages, in this case referred to as datagram, to other hosts on an Internet

Protocol(IP) network without prior communications to set up special transmission channels or data paths.

Transmission Control Protocol (TCP):

- The **Transmission Control Protocol** (**TCP**) is a core protocol of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as *TCP/IP*. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network. TCP is the protocol that major Internet applications such as the World Wide Web, email, remote administration and file transfer rely on. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability.

Software Tools

- **NS-2.28 software**:

A network simulator is software that predicts the behavior of a computer network. Network simulators serve a variety of needs. Network simulators are relatively fast and inexpensive.

OTCL Script Language :

Refers to an object oriented extension of Tcl in network simulator and usually run under Unix environment.

DOVE Controller:

Performs management & a portion of control plane functions
across DOVE Switches

DOVE Switches (DOVES):

–Provides layer-2 over UDP overlay (e.g. based on OTV/VXLAN)
–Performs data and some control plane functions
–Runs in Hypervisor vSwitch or gateways
–Provides interfaces for Virtual Appliances to plug into
(Analogous to appliance line-cards on a modular switch)

DOVE Technology + Multi-pathing :

DOVE network simplifies virtual machine network
–Enables multi-tenancy all the way to the VM
–Enables single MAC Address per physical server (2 for HA)
–Significantly reduces size of physical network TCAM & ACL tables
–Increases layer-2 scale within Data Center and across Data Centers,
by decoupling VM's layer-2 from physical network

Qbg automates layer-2 provisioning , DOVE automates layer 3-7 provisioning standards based multi-pathed physical network

Back-ups:

- Automating coordination of layer-2 state
- IBM DVS 5000v overview
- Examples of some of the values associated with DOVE Technology

–Multi-tenancy
–Efficiency

CONCLUSION

Data was broadcasted to a desired number of receivers for efficient privacy preserving and authentication was achieved using DOVE scheme. This allowed reduced time in sending of data to multiple receivers .

REFERENCE

[1] L. Roberts and B. Wessler, "Computer network development to achieve resource sharing," in *1970 Spring Joint Computer Conf., AFIPS Conf. Proc.*, vol. 36. Montvale, N. J.: AFIPS Press, 1970, pp. 543—549.

[2] L. Pouzin, "Presentation and major design aspects ofthe CYCLADES computer network," in *Proc. 3rd Data Communications Symp*., 1973.

[3] F. R. E. Dell, "Features of a proposed synchronous data network," in Proc. *2nd Symp. Problems in the Optimization of Data Communications Systems*, 1971, pp. 50—57.

[4] R. A. Scantlebury and P. T. Wilkinson, "The design of a switching system to allow remote access to computer services by other computers and terminal devices," in *Proc. 2nd Symp. Problems in the Optimization of Data Communications Systems*, 1971, pp. 160-167.

[5] D. L. A. Barber, "The European computer network project," in *Computer Communications: Impacts and Implications*, S. Winkler, Ed. Washington , D.C., 1972, pp. 192-200.

[6] R. Despres, "A packet switching network with graceful saturated operation," in *Computer Communications: Impacts and Implications*, S. Winkler, Ed. Washington, D.C., 1972, pp. 345-351.

[7] R. E. Kahn and W. R. Crowther, "Flow control in a resource-shaping computer network," *IEEE Trans. Commun.*, vol. COM-20, pp. 539-546, June 1972.

[8] J. F. Chambon, M. Elie, J. Le Bihan, G. LeLann, and H. Zimmerman, "Functional specification of transmission station in the CYCLADES network. STST protocol" (in French), I.R.I.A. Tech. Rep. SCH502.3, May 1973. © 1974 IEEE. Reprinted, with permission, from IEEE Trans on Comms, Vol Com-22, No 5 May 1974

[9] S. Carr, S. Crocker, and V. Cerf, "HOST-HOST Communication Protocol In the ARPA Network," in *Spring Joint Computer Conf., AFIPS Conf. Proc.*, vol. 36. Montvale, N.J.: AFIPS Press, 1970, pp. 589-597.

[10] A. McKenzie, "HOST/HOST protocol for the ARPA network," in *Current Network Protocols*, Network Information Cen., Menlo Park, Calif., NIC 8246, Jan. 1972.

[11] L. Pouzin, "Address format in Mitranet," NIC 14497, INWG 20, Jan. 1973.

[12] D. Walden, "A system for interprocess communication in a resource sharing computer network," *Commun. Ass. Comput. Mach*., vol. 15, pp. 221-230, Apr. 1972.

[13] B. Lampson, "A scheduling philosophy for multiprocessing system," *Commun. Ass. Comput. Mach*., vol. 11, pp. 347-360, May 1968.

[14] F. E. Heart, R. E. Kahn, S. Ornstein, W. Crowther, and D. Walden, "The interface message processor for the ARPA computer network," in *Proc. Spring Joint Computer Conf.*, *AFIPS Conf. Proc*., vol. 36. Montvale, N.J.: AFIPS Press, 1970, pp. 551-567.

[15] N. G. Anslow and J. Hanscoff, "Implementation of international data exchange networks," in *Computer Communications: Impacts and Implications*, S.

★★★