Hyper-encryption Scheme for Data Confidentiality in Wireless Broadband (WiBro) Networks

Md. Abdul Hamid[1], Choong Seon Hong[2]
[1,2]Dept. of Computer Engineering, Kyung Hee University
1, Seocheon, Giheung, Yongin, Gyeonggi, Korea, 449-701
hamid@networking.khu.ac.kr and cshong@khu.ac.kr

Abstract

We address the data confidentiality for wireless broadband (WiBro) networks. In WiBro, as the channel is wireless in nature, it suffers from passive and active attack. Passive attack, for example is to decrypt traffic based on statistical analysis and active attack is to modify traffic or inject new traffic from unauthorized mobile stations. Due to high mobility, frequent session key distribution is a bottleneck for the mobile stations. In aspect of WiBro, there is a communication between mobile station to base station, and also in mobile station to mobile station. It is expected to ensure data confidentiality while maintaining minimum overhead for the resource constrained mobile stations. In this paper, we proposed a security framework based on the concept of hyper-encryption to provide data confidentiality for wireless broadband networks.

1. Introduction

Development of mobile internet access has the growing demand for advanced multimedia data transfer. The standardized WiBro developed specially and particularly in South Korea is going to be commercialized in 2007. The advantages of integrating cellular with WiBro include high data rate, low cost, the ubiquity of hot spots and the offload of cellular spectrum. WiBro offers high speed data service within specific and usually small areas. A fundamental problem in cryptography is that of secure communication over an insecure channel [1] and hence, the primary goal of encryption is to protect the privacy of the conversation between communicating parties.

WiBro is to provide wireless internet access with PSS (Portable Subscriber Station) under the stationary and medium speed mobile environment. As it uses wireless medium, we can't consider it undoubtedly secured communication. We want to mean that the message transformation sometimes may not be appropriate as if it is a wireless channel. Therefore, system shall prohibit 3rd party's unlawful usage and unlawful access network service except lawful user and terminal. We focus our approach to devise a security scheme which conveys the data confidentiality.

WiBro will increase the market for broadband wireless access solutions by taking advantage of the inherent mobility of the wireless media. It is expected to fill the gap between very high data rate wireless local area networks and very high mobility cellular systems. In our scheme we mainly consider the message transformation between PSS to PSS. We present a scheme for efficient secure two party communications with provable everlasting security. The security framework proposed exploits the concept of hyper-encryption [1].

2. Proposed Scheme

For WiBro we consider the following protocol for ensuring its security especially on data confidentiality when mobile stations are occupied with information exchange. The mobile stations PSS (Portable Subscriber Station) which is under RAS (Radio Access Station) share secret key K. After the shared secret key is established, the random string is broadcast by the access control router (ACR), and the sender and the receiver produce a shared one-time pad, using the bits of determined by shared secret. Then, sender computes the ciphertext, and sends to receiver who decrypts by it to plaintext message. Simple bit-wise XOR operation is performed for encipher-decipher.

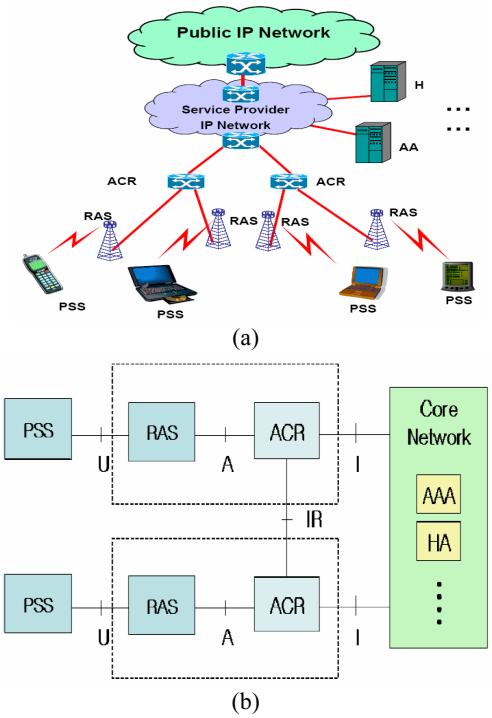

Fig. 1 Wireless Broadband: (a) Portable Network Architecture. (b) WiBro network reference model. RAS and ACR within the dotted line can be logically integrated as a single entity and is referred to as a wide-sense RAS (fig. source: [2]).

"This paper was supported by ITRC and MIC"

We assume that all the access control routers (ACRs) in WiBro environment are able to communicate and synchronize themselves to broadcast random bits and all the PSSs are able to hear those random bits.

Data/Message: $M = (M_1, \ldots\ldots, M_m) \in \{0, 1\}^m$
Random bits: $X = (x^{(1)}, \ldots\ldots, x^{(m)})$, $x^{(i)} \in \{0, 1\}^n$
Secret Key: $K = (k_1, \ldots\ldots, k_p) \in \{1, \ldots\ldots n\}^p$

Random bits X will be broadcasted in a considerable amount that is very large compare to shared secret key K. The message will be encrypted according to the following protocol:

1. *for i=1 to m do*
2. *for j=1 to n do*
3. *if $j \in K$ then*
4. *PSSs create a session key by using $S = f(x^{(i)}, k_{(j)})$*
5. *end for loop*
6. *Sender PSS encrypts $C = S \oplus M$ and sends C to receiver PSS*
7. *Receiver PSS decrypts $M = S \oplus C$*

We use the concept of matrix key-distribution [3] scheme to assign the shared secrets among the PSS units in the network. Any two nodes want to communicate will share the common secrets using the multiline matrix based key assignment.

This version is achieved by allocating more key lines to each node instead of only two as in the basic scheme. Assume there are N nodes where $N = m^2$. A communication map is defined as an m x m matrix on which each point has an address P_{ij} and corresponds to a node n_{ij}, where $i, j = 1, 2, \ldots, m$. A key map is also defined as an m x m matrix where point i, j corresponds to a key k_{ij}. The key set sent to node n_{ij} is

$K_{ij} = \{k_{xy} \mid y - j + c_L(x - i) = 0 \bmod(m)\}$,
$L = 1,2 \ldots\ldots z$, and $c_p \neq c_q$ *when* $p \neq q$.

The key set is a set of L lines on the key map all passing through point i, j. These keys can be stored in t tables where each entry is indexed by the value $x - i$. The control station generate generates m^2 random keys and puts one on each point on the key map.
To compute a pair-wise key, the control station takes two addresses on the communication map as input, say P_{ij} and P_{uv}, and solves $L(L - 1)$ linear equation groups, each of which has the form:

$y - j + c_p(x - i) = 0 \bmod(m)$
$y - v + c_q(x - u) = 0 \bmod(m)$
$p, q = 1, 2, \ldots, L$ *and* $p \neq q$.

The solution is:

$x - i = (c_q(i - u) + j - v)/(c_p - c_q) \bmod(m)$.

The solutions (x, y) are positions on the communication map of keys that mobile stations n_{ij} and n_{uv} have in common. Then it can calculate a session key from these keys. Each mobile station (PSS) gets $L\sqrt{N}$ secret keys from multiline matrix and the total number of keys generated by the controlling station is N.

3. Discussion

In conventional encryption scheme, if the secret key K is captured then the past secrets are revealed because of the advances in algorithm or computing technology. Thus if a security scheme that ensures that even if the present secret key K is captured, the past secrets (message) will not be revealed will significantly eliminate the weakness of conventional algorithm. Furthermore, simple cryptographic computation is expected that can make the user (i.e. Mobile station, PDA etc.) feasible to use the scheme. Hyper-encryption scheme [1] along with the multiline matrix key (shared session key) may satisfy such requirements. There is a need to study on the feasibility of how to efficiently broadcast random bits from which session key is generated.

One-time pad offers information theoretic secrecy, provided that for each transmission of a message, a new independent, uniformly random one-time pad is established between communicating entities [1]. Matrix-based key distribution takes the assumption that there is one node at each point on the communication map. A stronger security result may be achieved if empty points are allowed [3]. In fact, empty points may specially be allocated to enhance security. To make insider attacks more difficult, a concept of logical positions of communicating entities can be introduced. So, an entity is not simply its physical address, but can be assigned and changed by the key controlling station. Moreover, the frequency of key change is based on the security level desired.

4. Conclusion

We have introduced a security scheme for multi-media data confidentiality in Wireless Broadband networks. We have proposed that secret key can be generated exploiting the concept of multiline matrix key distribution and be used with the hyper-encryption scheme. Further research directions include a) How efficient and feasible broadcasting random bits X from Access Control Router (ACR), b) Comparison of security strength with other existing wireless schemes like WLAN, Cellular networks.

References

[1] Y. Aumann, Y. Z. Ding, and M. O. Rabin, "Everlasting Security in the Bounded Storage Model," IEEE Transactions on Information Theory, vol. 48, no. 6, June 2002.
[2] Panyuh Joo, "2.3 GHz Portable Internet (WiBro) Overview," IEEE L802.16-04/29, IEEE 802.16 Session #33, Seoul, Korea.
[3] Li Gong and David J. Wheeler, "A Matrix Key-Distribution Scheme," J. Cryptology (1990) 2:51-59.

1097