International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 1– No.3, February 2012 – www.ijais.org

A Novel Algorithm HSHA to Secure Wireless Ad hoc Network

Atul Patel
Charotar University of Science and Technology
CHARUSAT Campus
Changa

Paresh Virparia
Sardar Patel University
Vallabh Vidyanagar

Ruchi Kansara
Charotar University of Science and Technology
CHARUSAT Campus
Changa

ABSTRACT
Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. Here we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks — multiple routes between nodes — to defend routing against denial of service attacks. We use replication and new cryptographic schemes, such as **HSHA** Key cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework. It helps the network to let the intruder cannot access the packet without the proper authentication. Unauthorized user cannot access the packet. There are various consequences of this algorithm.

General Terms
Security, Algorithms, Communication

Keywords
Ad hoc network, Cryptography, Wireless network, Key Management

1. INTRODUCTION
Routing protocols are difficult to efficiently secure. An attacker may, for example, attempt to inject forged routing messages into the system, or may attempt to modify legitimate routing messages sent by other nodes. An attacker may also attempt to exploit mechanisms in the routing protocol, such as those intended to quickly spread new routing information, to instead consume large amounts of network and router resources. Even the addition of cryptographic mechanisms to a routing protocol may make the protocol vulnerable to such attacks, since traditional security mechanisms are generally expensive in terms of CPU time; an attacker may be able to cripple several routers simply by flooding each router with large numbers of randomly generated, forged routing messages, which then must be authenticated and rejected by the router, leading to a denial of service by consuming all router CPU time.

Several researchers have proposed secure network routing protocols, but most have used standard digital signatures to authenticate routing update messages [1], [2]. Similarly, in the area of secure multi hop wireless ad hoc network routing, most researchers use standard digital signatures to authenticate routing messages [3], [4]. Unfortunately, generation and verification of digital signatures is relatively inefficient, and it is thus challenging to design a scalable, efficient, and viable secure routing protocol based on such asymmetric cryptography.

2. RESEARCH ISSUES IN WIRELESS AD HOC NEWTORK SECURITY
The objective of this section is to review the main research domains in wireless and sensor networks security that have been addressed in the past years. This review can be used in two ways. First, it provides a good summary of recently published approaches and solutions to problems related to wireless security. Thus, anyone starting research in this domain will become a broad overview to the current state of the art in this area. Secondly, the overview provides detailed references to specific research item that also show open issues to be addressed in further work.

In particular, the following seven domains have been addressed:

Key management – Key management is still one of the most challenging issues in ad hoc networks. The question is how multiple nodes establish shared keys and how they can revoke keys if necessary.

Performance and scalability – Focusing on low resource sensor networks, the performance of secure communication protocols and cryptographic algorithms needs to be considered for developing practical secure applications.

Access control and authentication – Access control and authentication in wireless networks is difficult as usually no complex security architectures such as IPSec or Kerberos are available.

Security protocols – Agreement protocols, integrated reliability and security measures are needed in distributed low resource networks.

Routing and clustering – Ad hoc routing in wireless networks requires countermeasures against two different threats. First, selfish nodes exhaust resources from the entire network without delivering any service and, secondly, routing protocols can be attacked to eaves drop information packets.

Secure localization – Localization is a major research issue in ad hoc and sensor networks. If no security measures are integrated, this essential component cannot be trusted.

Intrusion detection – Attacks such as address spoofing, denial of service, and general misbehavior need to be detected early in order not to spend too many resources for transporting attack packets.

3. SECURITY PROTOCOLS

Wireless sensor networks are specific ad-hoc networks [5] with a larger number of nodes, a limited energy and a lower computing power. Looking at secure communication protocols, a number of evaluations have been published that focus on various aspects of communication in wireless and sensor networks. For example, the MAC layer security in 802.15.4 networks has been deeply investigated [6]. The unreliability of wireless communication has been continuously addressed in the wireless communications community. AN example for specific solutions that also incorporate security measures in this investigation is the reliable and semi-reliable communication with authentication (RAC) algorithm [7].

Computer network and information security has three aspects: security, attacks and security mechanisms. The objective of the security service is to achieve confidentiality, authentication, integrity, non-repudiation, access control, and availability. Cryptographic mechanisms include algorithms and keys [8]. Cryptographic algorithms consist of secret key algorithms and public key algorithms. In secret key algorithms, also called symmetric algorithms, the same secret key is used by the sender and the receiver e.g., Substitution cipher algorithm and Data Encryption Standards Algorithm etc. Public key algorithms, called asymmetric algorithms, use a related key pair, namely, a secret key and a public key e.g., RSA etc. The sender uses one from a key pair of a secret key and a public key, and the receiver uses another from the key pair. In public key algorithms, only a specific person (a sender or a receiver) knows a private key. On the other hand, persons in the networks may know more than one person's public key.

In the literature there are many cryptographic algorithms for Wireless Ad-hoc Network. Nitesh Saxena [9] has discussed the public key cryptography and certificates in ad hoc networks, with theoretical security issues. Dijiang Huang [10] describes the Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks. Cordasco et.al. [11] compares the security issues of cryptographic and Trust-based Methods for MANET Routing Security. Ching et.al. [12] investigated an identity-based broadcast encryption scheme for mobile ad hoc networks. Sheng et.al [13] focused on the enhanced security design for threshold cryptography in ad hoc network. Toh et.al. [14] has investigated the communication performance of wireless ad hoc networks, throughput and end-to-end delay of the networks. Santos et.al. [15] have analyzed the performance parameter throughput, average end-to-end- delay and collision with respect to mobility for vehicular mechanism ad-hoc networks. Woon et.al. [16] evaluates the performance of wireless 802.15.4 using simulation and test bed approach. Karyotis et.al. [17] have designed a novel framework mobile attach strategy modeling and vulnerability analysis in wireless ad hoc networks.

4. PROPOSED HIGHLY SECURED HIGHLY AVAILABLE (HSHA) KEY MANAGEMENT

The following algorithm describes the new way of implementing cryptography mechanism to wireless ad hoc network. In this algorithm, the key is generated dynamically at the time of datagram start and reach to the destination. We need not depend upon the neighboring node for the key. The datagram itself provide the encryption key. Here we are using the start time, the time at which the packet is forwarded. At each character, some manipulation has been done and a new character is formed. On the receiver end, the reverse process is done.

The main benefit of implementing this algorithm is that we need not to depend on the neighbor node for the key so the possibility of intruder is very less. Also there is no chance of illegal user as start time field is only available to the legal receiver end. If any intermediate node tries to access this field then it will be invisible and inaccessible for them.

Encryption (At Sender Side)

```
BEGIN

Key=0
IF StartTime.sec>24 THEN
        Key=(StartTime.sec/2)+(StartTime.sec%2)

        WHILE Not Key<24
            StartTime.sec=StartTime.sec/2

        Key=(StartTime.sec/2)+(StartTime.sec%2)
        END WHILE
ELSE
        Key=(StartTime.sec/2)+(StartTime.sec%2)

END IF

i=0
WHILE DATA IS NOT NULL

        IF key>24 then
                Key=1
        END IF
        DATA[i]=DATA[i]+key

        Key=key+1
        i=i+1
END WHILE

StartTime.Visible=FALSE
END
```

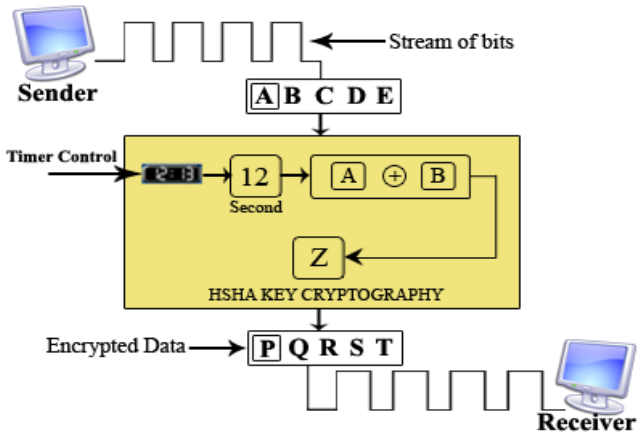

Fig 1: Encryption Sender Side

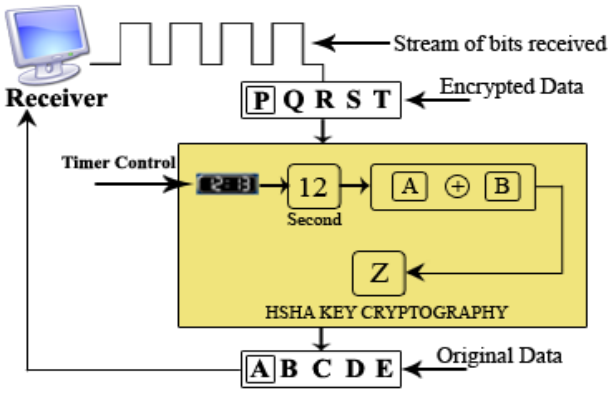

Fig 2: Decryption at Receiver Side

Decryption (At Receiver or Any Intermediate Node Side)

```
BEGIN
Key=0
IF this.DESTINATION=DESTINATION THEN
                StartTime.visible=TRUE
          IF StartTime.sec>24 THEN
               Key=(StartTime.sec/2)+(StartTime.sec%2)
   WHILE Not Key<24
        StartTime.sec=StartTime.sec/2
       Key=(StartTime.sec/2)+(StartTime.sec%2)
       END WHILE
 ELSE
       Key=(StartTime.sec/2)+(StartTime.sec%2)
        END IF
           i=0
        WHILE DATA IS NOT NULL
         IF key>24 then
             Key=1
        END IF
  DATA[i]=DATA[i]-key
        Key=key+1
         i=i+1
         END WHILE
           SOURCE.SendSuccessMessage()
      ELSE
           StartTime.visible=FALSE
       END IF
      END
```

To support this algorithm, we need to add two more fields in the IPv4 Data gram format. We require the start time of the packet and the reach time of the packet. So we are going to add two more fields in the IPv4.

The HSHA key management starts its work as soon as datagram leaves the sources address. It computes the key from the start time and the reach time using the mathematical formula. At each time it will be added to the Data key and encrypted form is generated. This process is continue until all the data are converted in to encrypted form. At the receiver side the destination address capture the start time and reach time compute the key and deduct the key value from the data value and get the original data. This process continues until all the data is decrypted.

The main intention of capturing the start time and estimated reach time is to compute key from that. These two fields are disables for others, only the destination address can access this field and compute the key and decrypt the data and get its original form back.

5. PROPOSED IPv4 DATAGRAM FORMAT

Header Contents:

Version: Version of the IP protocol which determines how to interpret the header. Currently the only permitted values are 4 (0100) or 6 (0110). The header format shown here is valid for IPv4 only.

IHL: Length of header as a number of 32-bit words

***Type of service*:** This field is often ignored by current routers but is meant to allow traffic to be prioritized (among other things).

***Total Length*:** The length of the entire datagram including header and data: maximum permitted it 65,535 bytes or 64K. Identification, Flags and Fragment Offset: These values allow datagram to be fragmented for transmission and reassembled at the destination

***Time to live*:** An integer which is decremented at each router "hop"; supposed to be interpreted as a number of seconds but more often treated as a "hop count". If the value reaches zero, the datagram is discarded and an ICMP message is sent to the source host.

***Protocol*:** Identifies the transport-layer protocol which will interpret the Data section. This will typically be TCP or UDP but other values are possible. Protocols are identified by a unique number.

***Header checksum*:** This is used to verify the header, and is recomputed at each router hop. This field is left out of IPv6 which relies on the transport layer for verification.

***Addresses and Options*:** These are 32-bit IP addresses which identify the network and host address. Note that IP does not have to specify addresses of any intermediate nodes; this can be left to the router. Routing requirements can also be specified in the Options field, along with options to do with security and debugging.

***Start Time*:** This is the 16 bit timer field which store the time at which packet leaves from the server or sender side.

***Reach Time*:** This is the estimated time at which the packet is supposed to reach at the destination side or receiver side.

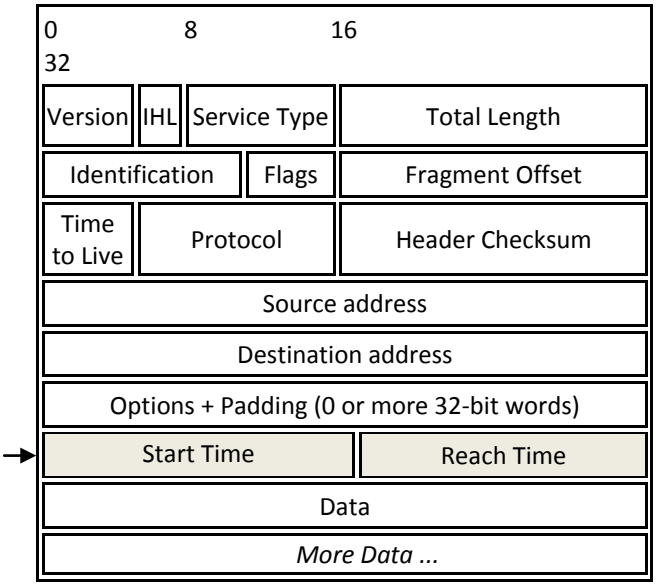

Fig 3: IPv4 new Datagram Format

This is the new IPv4 datagram format which is required to change in order to generate the key dynamically using the fields start time and reach time. So one must not rely on the neighbor ring node. No intermediate node or responsible host is required to hold the key. As mention in the algorithm, the key will be generated from the start time so the datagram itself generating the key dynamically. In this case, we prevent our computer from intruder as no intermediate responsible is required.

6. CONCLUSION

Any system, on the network, needs security in terms of secure routing, cryptography, authentication, data confidentiality, data integrity, data freshness, non-repudiation, data redundancy etc. They are analyzed to try to solve all these problems by means of new cryptography algorithm HSHA. Still efforts are made to make algorithm more efficient.

Also the algorithm will be implemented and analyzed for various consequences and outcomes. Further efforts are to be done to set up these security mechanisms in an ad hoc network and to investigate the impact of these security mechanisms on the network performance.

7. REFERENCES

[1] Stephen Kent, Charles Lynn, Joanne Mikkelson, and Karen Seo. Secure Border Gateway Protocol (S-BGP) . Real World Performance and Deployment Issues. In Proceedings of the 2000 Symposium on Network and Distributed Systems Security (NDSS '00), pages 103.116, February 2000.

[2] Jiejun Konh, Petros Zerfos, Haiyun Luo, Songwu Lu, and Lixia Zhang. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. In Proceedings of the Ninth International Conference on Network Protocols (ICNP'01), pages 251.260, November 2001.

[3] Bridget Dahill, Kimaya Sanzgiri, Brian Neil Levine, Elizabeth Royer, and Clay Shields. A Secure Routing Protocol for Ad hoc Networks. In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP '02), November 2002.

[4] Manel Guerrero Zapata and N. Asokan. Securing Ad Hoc Routing Protocols. In Proceedings of the ACM Workshop on Wireless Security (WiSe 2002), September 2002.

[5] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless adhoc networks: a survey. Comput. Netw. 2002; 38(4):393–422, doi:http://dx.doi.org/10.1016/S1389-1286(01)00302-4.

[6] V. B. Misic, J. Fung, and J. Misic. MAC Layer Security of 802.15.4-Compliant Networks. In 2nd IEEE International Conference on Mobile Ad Hoc and Sensor Systems (IEEE MASS 2005): International Workshop on Wireless and adhoc Networks Security, Washington, DC, USA, November 2005.

[7] F. Dressler. Reliable and Semi-reliable Communication with Authentication in Mobile Ad Hoc Networks. In 2nd IEEE International Conference on Mobile Ad Hoc and Sensor Systems (IEEE ASS 2005): International Workshop on Wireless and adhoc Networks Security, pages 781–786, Washington, DC, USA, November 2005.

[8] Izhak Rubin, Runhe Zhang, "Adhoc Robust throughput and routing for mobile ad hoc wireless networks", Ad Hoc Networks Elsevier Volume 7, Issue 2, March 2008, Pages 265-280.

[9] Nitesh Saxena, "Public Key Cryptography Sans Certificates in Ad Hoc Networks", ACNS 2006, LNCS 3989, pp. 375-389.

[10] Dijiang Huang, "Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks", Int. J. Security and Networks, Vol. 2, Nos. 3/4, 2007 pp272-283.

[11] Jared Cordasco, Susanne Wetzel, "Cryptography vs. Trust-based Methods for MANET Routing Security", Electronic Notes in Theoretical Computer Science TM 2007.

[12] Ching Yu Ng, Yi Mu, and Willy Susilo, "An identity-based broadcast encryption scheme for mobile ad hoc networks", Journal of Telecommunication and Information Technology, 1/2006, pp 23-29.

[13] Sheng-Ti Li, Xiong Wang, "Enhanced Security Design for Threshold Cryptography in Ad Hoc Network", NEW2AN 2004, St.Petersburg,Russia, pp27-31.

[14] C.K. Toh, M. Delwar, D. Allen, "Evaluating the communication performance of an ad hoc wireless network", IEEE Transactions on Wireless Communications 1 (3) (2002), pp 402-414.

[15] A. Santos, A. Edwards, R.M. Edwards, N.L. Seed, "Performance evaluation of routing protocols in vehicular ad-hoc networks", International Journal of Ad Hoc and Ubiquitous Computing 2005 - Vol. 1, No.1/2 pp. 80 – 91

[16] Wilson T.H. Woon, Tat-Chee Wan, "Performance evaluation of IEEE 802.15.4 wireless multi-hop networks: simulation and testbed approach", International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC) Volume 3 - Issue 1 - 2008, pp57 - 66.

[17] Vasileios Karyotis, Symeon Papavassiliou, Mary Grammatikou, Vasilis Maglaris, "A novel framework for mobile attack strategy modeling and vulnerability analysis in wireless ad hoc networks", International Journal of Security and Networks 2006 – Vol. 1, No.3/4 pp. 255-265.