ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

TLS: Improving Security for Ad-Hoc Networks using Three Level Security Mechanism

R.Murugesan*, Dr M Vijayaraj

*Associate Professor, ECE Department, Bharath Niketan Engineering College, Aundipatty, India

Professor,ECE Department, Government College of Engineering, Tirunelveli, India

rmurugesan61@gmail.com

Abstracts

A group of large autonomous wireless nodes are connected and communicating in a P2P method on a Heterogeneous environment without defined infrastructure is named Mobile Ad-hoc network. Various mechanisms and techniques are applied for providing security for Ad-Hoc networks and a major problem MANON was analyzed in the existing system which is providing good performance where the network size is small. In this paper a Three Level Security mechanism is proposed for malicious behavior detection by 1. Confidentiality, 2. Data integrity and 3. Certified Conformation. The TLS approach will be evaluated using NS2 – [Network Simulator] to provide and whether nodes in the Ad-Hoc networks are malicious or not. The simulation results show the performance of the proposed approach.

Keywords: Ad-Hoc Network; Security in Ad-Hoc Network; Confidentiality; Data Integrity; Data-Availability.

Introduction

An ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructureto keep the network connected. Ad hoc networks can be formed, merged togetheror partitioned into separate networks on the fly, without necessarily relying on a fixed infrastructure to manage the operation. Nodes of ad hoc networks are often mobile, whichalso implicates that they apply wireless communication to maintain the connectivity, inwhich case the networks are called as mobile ad hoc networks (MANET). Mobility is not,however, a requirement for nodes in ad hoc networks, in ad hoc networks there may existsstatic and wired nodes, which may make use of services offered by fixed infrastructure.

Ad hoc networks may be very different from each other, depending on the area of application: For instance in a computer science classroom an ad hoc network could be formedbetween students' PDAs and the workstation of the teacher. In another scenario a groupof soldiers is operating in a hostile environment, trying to keep their presence and missiontotally unknown from the viewpoint of the enemy. The soldiers in the group work carrywearable communication devices that are able to eavesdrop the communication betweenenemy units, shut down hostile devices, divert the hostile traffic arbitrarily or impersonatethemselves as the hostile parties. As can obviously be seen, these two scenarios of adhoc networking are very different from each other in many ways: In the first scenario themobile devices need to work only in a safe and friendly environment where the networking conditions are predictable. Thus no special security requirements are needed. On theother hand, in the second and rather extreme scenario the devices operate in an extremely

Related works

A detailed literature survey is given in this section for providing better security than the existing approaches comparatively. In [1], a mutual trust among the nodes using digital signature verification is applied under AODV protocol for providing security in node level. A security aware ad-hoc routing is proposed is proposed to provide security in route discovery and checks the security metrics to validate the protocol. A safety communication in a valid route is established in ad-hoc network [2]. An identification of protection issued relevant to problems, is investigated and recovered in [3]. MeEliece algorithm is introduced to provide security which uses Dispense Key as distributed for the entire network [4]. This key used for authentication as well as data encryption and decryption. Various drawbacks of previous researches is analyzed and finally the author giving various solutions for the issues on VANET [5].

In [6]the author presents the brief study about the wireless protocols for secure routing as well as protocols for securing packets transmission. This paper describes the limitations and the characteristics for each protocol and attributes.In paper [7], the special navigation scheme proposed to guide the vehicle drivers to desired destinations. The advantage

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

of proposed scheme is that, it using real time road conditions. The author proposed an optimized traffic masking algorithm. It removes any leaking in [8]. A method to find the DOS attacks in VANETs is proposed. This paper focused on the jamming of beacons in [9]. Various challenge of power control and channel selection is analyzed. [10]. Authorin [11] presents an efficient authentication scheme for vehicular and ad hoc networks. The existing schemes have a disadvantage of long computation delay in CRL and signature verification process cause high message loss.

Problem statement

Since nodes in the ad-hoc networks are self adaptive, dynamic and random in nature, the vulnerability of the ad-hoc nodes increasing gradually. Due to node vulnerability the ad-hoc network needs a permanent and best solution for secured communication.

Proposed approach

To provide better solution for the problem found in this paper, a three level security approach is applied in the ad-hoc network and it is discussed very clearly in this section.

TLS brings security in three ways like confidentiality, data integrity and data availability. The confidentiality makes authentication and authorization based security for entire nodes in the network. The data integrity makes combining the data packets from the source node from various paths to destination and the data received acknowledgements is generated and send to source node. Once the confidentiality is valid, the source node sends data packets to the next hop in the route to the destination. While transmitting the data packets the next-hop key is verified and validated. Finally at destination node, the data packets from various sources and through various routes will be collected and integrated. The data collection and integration will be carrying out on the destination with the help of data integrity. The data integrity can be obtained by comparing the data packet's unique header information with the TTL – [Time to Leave] to avoid conflicts on the data integrity. After the data integrity the destination node should prepare a data conformation certificate provides Acknowledgement about the data received from the particular source via particular route.The TLS system model is shown in the following figure-1 for better understanding the functionality of the TLS approach.

Network model

An ad-hoc network G is constructed using N number of nodes and the nodes are deployed randomly and dynamically. It is also assumed that the BS is assigning the keys for entire nodes in the network. The topological structure used in TLS is shown is Figure-1. TLS functionality defined in three levels and they are:

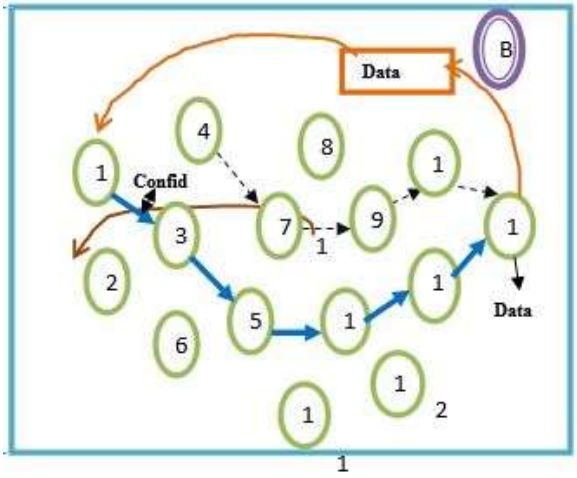

Figure-1: Proposed System Model based Ad-hoc Network

Confidentiality

Entire node in the network is assigned by a dynamic key generated randomly and assigned by the Base Station – [BS]. The key is generated using the Equation-[1]

$$\boldsymbol{Key(Node_i) = randint(i) * (N)} \quad -- \quad - \quad Equation[`1]$$

The key of ith is generated using the random value of i multiplied by the number of nodes N in the network G.

Data-Integrity

The data packets received in the destination is collected in each route and group it. While grouping

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

the data packets, the packets header information is analyzed to verify the source-ID, TTL and hop-ID and is depicted in Figure-2.

PNO	SID	TTL	HID	..	..	..	RID

Figure-2: Packet Format

The first column contains sequence number of the packets,the second column contains the source-ID, the third column contains the time to leave of the packet and the fourth column contains the hop-ID 1, then hop-ID2 etc. Where the last column contains the route-ID in which the data packet is transmitted. In the destination all the packets are received and they are cloned due to PNO, source-ID and route-ID. For example from route 1, the source node is 1, packet numbers from 1 to M are cloned as the data. It is also easy to verify that packet missing in this approach with the help of the packet number.

Certified Conformation

One the data integrity is achieved successfully the destination node generates a data conformation certificate and send directly to the source node to conform that the particular source node's data is received successfully. The conformation certificate contains the total number of packet received and the time of receive.

TLS_Algorithm ( )

{

- ***Construct the Network***
  - ***Make Random Deployment***
- ***Generate random keys***
  - ***Assign keys to entire nodes in the network***
- ***Transmit data from source to destination in c***
- ***Verify the keys of each hop***
- ***Verify the data packet format***
- ***Data collection and certificati***

}

The TLS algorithm is written in TCL – [Transmission Control Language] and deployed in network simulator with AODV routing protocol. The simulations carried out and verify the performance of the TLS is evaluated by applying various numbers of nodes in different rounds.

Simulation settings

To check the performance evaluation of the proposed approach the TLS is written in TCL code based on Network Simulator platform version-2. The following Table-1 shows the parameter settings given in NS2.

Parameter	Value
Area	1200 x 1200
Number of Nodes	20
Routing Protocol	AODV
Language	TCL, C++
Propagation Model	Two ray ground
MAC	IEEE-802.11
	and etc.

Results and discussion

In the simulation 20 nodes is deployed in a 1200 x 1200 size network and the throughput, delay and energy of the proposed approach is computed using awk scripts and compared with the existing MANON approach. The results are shown in the form of graph and showing that the TLS approach is efficient than the existing approach MANON is depicted clearly in Figure-3, Figure-4 and Figure-5 respectively.

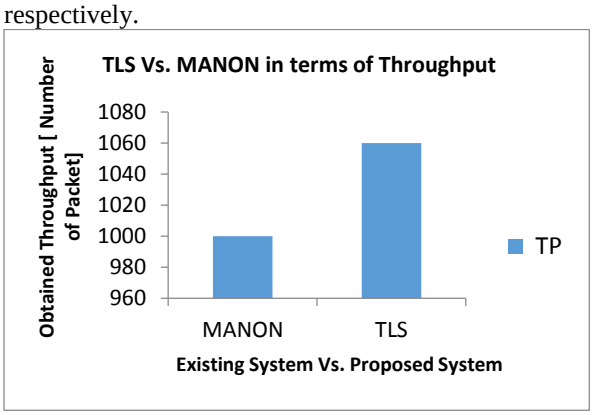

Figure-3: Throughput Comparison TLS vs. MANON

The throughput of the proposed approach is better than the existing approach where for 20 nodes MANON obtained 1000, and TLS obtained 1060.

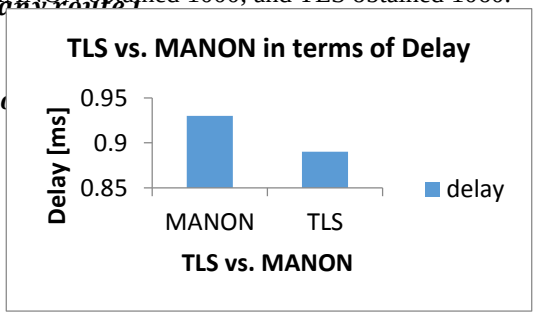

Figure-4: Delay Comparison TLS vs. MANON

The time delay taken by the proposed approach is less than the existing approach where for 20 nodes MANON taken0.93ms, and TLS taken 0.89ms.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

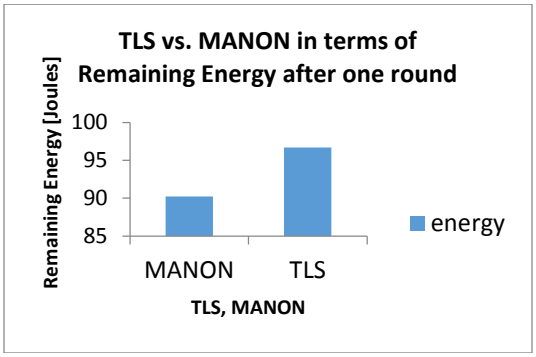

Figure-5: Energy Comparison TLS vs. MANON

The energy save by the proposed approach is greater than the existing approach where for 20 nodes MANON spent 9.77%, and TLS spent 3.3% joules of energy.

Conclusion

The TLS provides a highest security than the existing MANON approach and the approach affecting the QOS factors to be considered for performance evaluation. From the results and discussion, it is clear that TLS approach is efficient than the existing approaches.

References

1. Tarun Kumar Mishra, Bhupendra Singh, Arun Kumar, "A Security Scheme for Mobile Ad-hoc Network with Reduced Routing Overhead ",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013.
2. Seung Yi, Prasad Naldurg, Robin Kravets, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks".
3. Dr. Anna SaroVijendran , A. Kamatchi, "A SURVEY ON SECURITY IN MOBILE ADHOC NETWORK", International Journal Of Engineering And Computer Science ISSN:2319-7242 ,Volume 2 Issue 4 April, 2013 Page No. 1384-1393.
4. Suma Christal Mary, S., M. PallikondaRajasekaran and Y. ChrisbinJeeva, "A NOVEL APPROACH FOR INFORMATION SECURITY IN AD HOC NETWORKS THROUGH SECURE KEY MANAGEMENT", Journal of Computer Science 9 (11): 1556-1565, 2013.
5. AnkitaAgrawal, AditiGarg, NiharikaChaudhiri, Shivanshu Gupta, DeveshPandey, Tumpa Roy, "Security on Vehicular Ad Hoc Networks (VANET) : A Review Paper ",International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 1, January 2013.
6. SalwaAqeel Mahdi, Mohamed Othman, Hamidah Ibrahim, Jalil Md. Desa and JumatSulaiman; "PROTOCOLS FOR SECURE ROUTING AND TRANSMISSION IN MOBILE AD HOC NETWORK: A REVIEW"; Journal of Computer Science 9 (5): 607-619, 2013.
7. T.W. Chim, S.M. Yiu, Lucas C.K. Hui, and Victor O.K. Li, "VSPN: VANET-Based Secureand Privacy-Preserving Navigation", IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 2, FEBRUARY 201
8. Alfonso Iacovazzi and Andrea Baiocchi, "Internet Traffic Privacy Enhancement withMasking: Optimization and Tradeoffs", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014
9. Nikita Lyamin, Alexey Vinel, Magnus Jonsson, and Jonathan Loo, "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks", IEEE COMMUNICATIONS LETTERS, VOL. 18, NO. 1, JANUARY 2014
10. Luca Rose, Samir M. Perlaza, Christophe J. Le Martret, and M´erouaneDebbah, "Self-Organization in Decentralized Networks: A Trial and Error Learning Approach", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 13, NO. 1, JANUARY 2014
11. Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, and Hui Li, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 63, NO. 2, FEBRUARY 2014.