ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

An Investigation Study on Secured Data Communication in Mobile Ad-hoc Networks

S.Sangeetha[#1], Dr.S.Sathappan[*2]

[#1]*Research Scholar, Department Of Computer Science, Erode Arts and Science College, Erode, Tamil Nadu, India*
[*2] *Associate Professor, Department of Computer Science, Erode Arts and Science College, Erode, Tamil Nadu, India*

[1] sgeethact2k7@gmail.com
[2] devisathappan@yahoo.co.in

***Abstract*— Anonymous routing protocols are significant in MANETs to present secure communications by hiding node individuality and avoiding the traffic attacks from observers. A trust-based routing protocol was designed in Mobile Ad-hoc Network (MANET) to route the messages through trusted nodes. It also used to reduce the dropping probability and improve network performance with throughput and packet delivery ratio. However, the intermediate nodes are difficult to identify the attack behaviour that increases the computational complexity. Cryptographic approach was provided for ensuring security among the mobile nodes in MANET for accomplishing efficient routing and data integrity. However, cryptographic operations are needed to recover the transient secrets in between multiple rounds of secure data forwarding across the routing path of MANET. In this paper we investigate and analyse certain number of existing protocols in Mobile Ad-hoc Network (MANET).**

***Keywords* — Anonymous routing protocols, trust-based routing protocol, Cryptographic approach, Mobile Ad-hoc Network (MANET).**

I. INTRODUCTION

A Mobile Ad- hoc Network (MANET) is a self-configuring, lack of infrastructure network of mobile devices joined without the wires. All devices in a MANET move in any direction and alter the connection to other devices. The hosts are linked by wireless links and the combination forms an arbitrary topology. The routers moves and systematizes arbitrarily, so the network's wireless topology alters quickly and randomly. MANETs group in the emergency situation for provisional actions or if there are no sources to gather the complicated networks. The network functions without any fixed infrastructure makes easy to organize. But, because of the lack of any fixed infrastructure, it is developed into complex one to utilize the routing techniques for network services, and contains number of issues in guaranteeing the security of the communication.Cryptographic approach was provided for ensuring security among mobile nodes in MANET for accomplishing efficient routing and data integrity. The cryptographic mechanisms ensure secured data forwarding on secured route path to corresponding destination mobile nodes. Cryptographic authentication protocol was used to provide efficient communication security between the mobile nodes in Ad-hoc network. Password-based authentication protocol was used for providing data security in mobile node data forwarding. Aggregated-proofs were identified for multiple malicious target nodes to achieve secured backward and forward anonymous data transmission.

II. LITERATURE SURVEY

Yanru Zhang et al [6] presented a Social-aware approach for optimizing Device-to-device (D2D) communication in wireless network with two layers called social network layer and physical wireless network layer. The social relations between individuals tend to be stable over time and it was used to achieve stable transmission link with D2D communication. However, in Mobile Ad-hoc Network scenario, D2D (mobile node to mobile node) need to provide neighbour mobile node data transmission services that are typically handled with secured data communication.

RACE, a report-based payment scheme was presented by Mohamed M.E.A Mahmud [7] for multi-hop Wireless networks to increase the cooperation between nodes, control of packet transmission and implement equality. RACE recognizes the cheating nodes with their evidences. Evidence aggregation technique was designed to minimize the storage space. However, the intermediate nodes fail to provide evidences because of computational complexity. Cipher XRay- a binary analysis framework [10] was designed to identify and to recover the cryptographic operations in wireless network data communication.

Derived from the avalanche effect of cryptographic functions, Cipher XRay pinpoints the boundary of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

cryptographic operation exactly and improves truly transient cryptographic secrets. But, cryptographic operations are not able to recover the transient secrets in between many rounds of cryptographic operations. To secure under many real-world attacks including key loggers and to obtain the information for protocols namely one-time-password protocol and password-based authentication protocol were designed by DaeHunNyang, Aziz Mohaisen., and Jeonil Kang [11]. But, with human interaction in authentication protocols, it was complex to provide authentication security because of their restricted ability of computation and memorization.

Anonymous Location-based Efficient Routing protocol (ALERT) is provided route anonymity, identity and location anonymity of source-destination node pair in wireless network were designed by HaiyingShen, and Lianyu Zhao [8]. ALERT does not allows timing attacks due to its non-fixed routing paths for a source destination pair. ALERT divides the network field into zones and selects nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. ALERT attains route anonymity protection and lower cost other anonymous routing protocols. ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol. But, ALERT is not completely foolproof to data falsification attacks. Efficient and Privacy-Aware Data Aggregation in Mobile Sensing were developed by Qinghua Li, Guohong Cao et al [1] with Sum aggregation protocol in to support large plaintext space for secured sensed data aggregation in mobile sensor networks. Sum aggregation protocol uses an additive homomorphic encryption and a key management technique to achieve the Min aggregate of time-series data. But, the sum aggregation protocol exposes the derivative data of the mobile node and the adversary which arrive the data value of particular mobile node in communication.

A. *Related Work*

Hyo Jin Jo et al [12] presented a three-round anonymous roaming protocol [12] used a pseudo-identity-based sign cryption scheme to perform efficient revocation with short revocation list and efficient authentication in wireless mobile networks. Three-round anonymous roaming protocol was evaluated with Canetti-Krawczyk (CK) model for better authentication among the mobile node communication. Anonymous roaming protocol fails to protect private keys and session keys of roaming users. To provide efficient wireless network communication security to all mobile nodes without trusted third party, a Private Circular Query Protocol (PCQP) was designed by Ting Lien [2] with Secret Circular Shift for Nearest Neighbour (NN) Search. PCQP protocol contains a space filling curve and a public-key homomorphic cryptosystem. But, LBS get ambiguity in identifying the information about mobile node on high speed wireless network. The security and accuracy rate in NN query were not jointly addressed.

A cryptographic provenance verification approach [11] enhances the assurance of data security in mobile host node by preventing and identifying malware activities in the wireless data traffic network. The cryptographic provenance verification approach with keystroke integrity services uses the hardware Trusted Platform Module (TPM) to handing host based secured traffic-monitoring in wireless network. However, outbound packets in the data traffic fail to contain equivalent proofs instantly after the malware were designed.

In VANET, the communications between the vehicles are made with each other and with roadside units (RSDs). Service oriented vehicular networks based handover scheme were designed by Khaleel Mershad and Hassan Artail [9] used in VANETs support many infrastructure-based commercial services. The success of data acquisition and delivery systems depends on the ability to defend against the different types of security and privacy attacks. However, the vehicular node unable to check dynamic road condition on the mobility of vehicles to handle the malicious messages being transmitted to RSUs in the network.

The aggregated-proofs are established for multiple targets to achieve backward and forward anonymous data transmission for the mobile nodes in the internet of things network by using Aggregated-Proof based Hierarchical Authentication scheme (APHA) was designed by Huansheng Ning [4]. Directed path descriptors, homomorphism functions, and Chebyshev chaotic maps are jointly applied for mutual authentication. APHA has security defects in terms of message interception by adversaries in Internet of Things (IoT) applications. Ning Wang, Ning Zhang [5] presented a secure secret key agreement protocol with three-node cooperative wireless communication system over block-fading channels. The key agreement scheme achieves a positive secret key rate even when an adversary has more favorable channel conditions. Key agreement protocol evaluated the lower bound using only by minimization function, which cause other channel noise exploitation by adversaries.

III. SECURED DATA COMMUNICATION IN MOBILE AD HOC NETWORKS

The communication in mobile Ad hoc networks has two phases. They are: the route discovery and the data transmission. In atmosphere, both phases are vulnerable to a many attacks. Initially, adversaries interrupt the route discovery by impersonate the destination with corrupted routing information or by disseminating forged control traffic. The attackers thwart the propagation of legal route control traffic and control the knowledge of nodes. Adversaries also interrupt the data transmission phase and acquire data loss

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

through illegally redirecting, dropping data traffic or inserting forged data packets. The secure routing protocols guarantee the exactness of the determined information not by themselves ensures the secure and undisrupted delivery of transmitted data.

A. Social Network Aware Device-to-Device Communication

The new mechanism called D2D communication mechanism is designed to develop the social network features for improving the packet transmission and to minimize the D2D communication is a capable technique for increasing the frequency resource usage efficiency and for offloading cellular network traffic. D2D communication distributes the same frequency band as cellular communication where resource allocation mechanisms are essential. The utilization of D2D is used to improve resource utilization and preserve an effective co-existence between the D2D services and the main cellular network.

B. Secure Payment Scheme with Low Communication and Processing Overhead for Multi hop Wireless Networks

A Report-based pAymentsChemE (RACE) is designed for Multi hop Wireless Network's. The nodes submit lightweight payment reports to the AC to modernize their credit accounts and store unchanged security tokens called Evidences. The reports consist of alleged charges and incentives of sessions without security proofs. The Accounting Center (AC) authenticates the payment by the reliability of the reports and clears the payment of the fair reports without cryptographic operations or computational overhead. In RACE, Evidences are presented and the AC relates cryptographic functions to authenticate while cheating, nodes submit security tokens. AC applies cryptographic functions to authenticate the payment in the receipt based schemes.

RACE is the initial scheme to authenticate the payment by studying the consistency of the nodes reports without presenting and processing the security tokens. RACE is the initial technique that employs the idea of Evidence to protect the payment and needs cryptographic operations in clearing the payment while cheating.

C. Key logging-resistant Visual Authentication Protocols

For security and usability two visual authentication protocols are designed. They are: one for password-based authentication, and the other for one-time-password. The protocols are safe under real-world attacks with key loggers. The protocols provide the merits because of visualization with security and usability. Prototype implementation with Android applications reveals the usability of protocols in real-world usage settings.

In addition, the design fails to require an explicit channel connecting the bank and the smart phone that are attractive. The smart phones are changed with the required functionality of capture photos. The property allows developing authentication protocols into the service context with smart wearable devices.

The following Table 3.1 represents the comparison of RACE, D2D communication, Sum aggregation protocol, Authentication protocol with their characteristics, merits and demerits.

TABLE 3.1
COMPARISON OF RACE, D2D COMMUNICATION, SUM AGGREGATION PROTOCOL, AND AUTHENTICATION PROTOCOL

PROTOCOLS	CHARACTERSTICS	MERITS	DEMERITS
RACE	Report-based payment scheme for multi hop wireless networks increases node cooperation, regulate packet transmission and enforces fairness. RACE detects cheating nodes with few Evidences	Evidence aggregation technique reduces Evidences' storage area RACE requires less communication and processing overhead	The intermediate nodes cannot compose Evidences Evidences is infeasible for calculation
D2D Communication Mechanism	D2D communication mechanism uses social network characteristics for increasing packet transmission and decreasing the load on network's infrastructure.	D2D provide proximity services in short-range technology. D2D communication over cellular has benefits over Wi-Fi in exact locations and situations.	In D2D communication, Wi-Fi does not available at all places Only cellular access is possible.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

	D2D communication increases spectral use of wireless systems and introducing new applications like proximity services or public safety applications.		
Sum Aggregation Protocol	Protocol uses sum aggregate of time-series data in un trusted aggregators. Privacy-preserving solution for Minimum of time-series data in mobile sensing user-to-aggregator communication	A sum aggregation protocol reduce the communication cost Sum aggregation protocol has lower communication overhead	The sum aggregation protocol does not expose the derivative data of any user The aggregator cannot know the data value of any particular user.
Authentication Protocols	Authentication protocols use visualization through augmented reality for achieving security and usability.	Authentication protocols provide high security and high usability Protocols increases the user experience and stops challenging attacks like key logger and malware attacks	Authentication protocols using human guidance is not easy because of limited capability of computation and memorization.

Comparison of various Parameters and Protocols

In addition to that the above said algorithm are analysed based on the parameters Execution Time, Throughput and Packet Delivery Ratio. RACE algorithm gives Poor performance in Execution Time when compared with the other algorithms D2D Communication Mechanism, Sum Aggregation Protocol, Authentication Protocols. Among the algorithms, the algorithm sum Aggregation protocol gives better result in Execution Time. Whereas in Throughput, Authentication protocol gives better result when compared to other protocols. But Sum Aggregation protocol gives Poor Performance. Based on Packet Delivery Ratio, D2D Communication protocol performs very well when compared to other protocols. The performance of RACE protocol is very poor in Packet Delivery Ratio.

IV. CONCLUSIONS

In this survey, comparison of RACE, D2D communication, Sum aggregation protocol, and Authentication protocol is carried out. We analysed their characteristics, merits and demerits in mobile ad-hoc network. In addition to that the protocols are analysed based on certain parameters such as execution time, throughput and packet delivery ratio. In future the performance of mobile Ad-hoc network can be improved by using B+ Tree Indexed Key and Quantum Key Authentication.

REFERENCES

[1] Qinghua Li, Guohong Cao, and Thomas F. La Porta, "Efficient and Privacy-Aware Data Aggregation in Mobile Sensing", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 2, MARCH/APRIL 2014

[2] Ting Lien, Yu-Hsun Lin, , Jyh-RenShieh, and Ja-Ling Wu, "A Novel Privacy Preserving Location-Based Service Protocol With Secret Circular Shift for -NN Search", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 6, JUNE 2013

[3] JunbeomHur., and Kyungtae Kang., "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO 1, FEBRUARY 2014

[4] HuanshengNing., Hong Liu., and Laurence T. Yang., "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO: 3, MARCH 2015

[5] Ning Wang, Ning Zhang, and T. Aaron Gulliver, "Cooperative Key Agreement for Wireless Networking: Key Rates and Practical Protocol Design", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 2, FEBRUARY 2014

[6] Yanru Zhang, Erte Pan, Lingyang Song., WalidSaad, Member, ZaherDawy, and Zhu Han., " Social Network Aware Device-to-Device Communication in Wireless Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 14, NO. 1, JANUARY 2015

[7] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) [1]Shen, "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO : 2, FEBRUARY 2013

[8] HaiyingShen, and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, JUNE 2013

[9] KhaleelMershad., and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO: 2, FEBRUARY 2013

[10] Xin Li., Xinyuan Wang., and Wentao Chang., "CipherXRay: Exposing Cryptographic Operations and Transient Secrets from Monitored Binary Execution", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 2, MARCH/APRIL 2014

[11] DaeHunNyang, Aziz Mohaisen., Jeonil Kang, "Keylogging-resistant Visual Authentication Protocols", TRANSACTIONS ON MOBILE COMPUTING, VOL. 1, NO. 8, AUGUST 2014

[12] Hyo Jin Jo, Jung Ha Paik, and Dong Hoon Lee., "Efficient P rivacy-Preserving Authentication in Wireless Mobile Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO: 7, JULY 2014

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

[13] KuiXu, HuijunXiong, Chehai Wu, Deian Stefan, and Danfeng Yao, "Data-Provenance Verification For Secure Hosts", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO: 2, MARCH/APRIL 2012.