A XTC based Authentication Scheme for MANET

Anshul Oza
Department of CSE
SVVV, Indore, India

Madhavi Bharani
Department of CSE
MIST, Indore, India

Gagan Shukla
Department of CSE
MITM, Indore, India

ABSTRACT
Security Mechanism based on Threshold cryptography that are been implemented for Mobile Ad-hoc Network normally have its own disadvantages or limits. As there should be at least the minimum number of nodes as per been declared in the threshold value to make the system running but there not always the number of nodes according to the threshold value so there is always a chance that system does not work even there is just a single node less than the threshold and even the system is not been compromised that problem can be solved using extended threshold cryptography(XTC). This paper concentrates how to provide a more secure mechanism in MANET using XTC.

General Terms
Wireless Sensor Network, Authentication, Cryptography

Keywords
MANET, Exteneded Threshold Cryptography, Key Generation

1. INTRODUCTION
Mobile ad hoc network is a decentralized and self-organizing network technology. With this network the devices are communicating using the wireless connectivity. All the nodes in network can move anywhere in network.The network topology is changing continuously due to node mobility and routing protocols are arranging the routes between communicating parties. Accordingly network follows the multi-hop options for transmission of data from source node to target node. Procedure of multi-hop communication states that data passes through the intermediate routers, between source and destination a malicious host can also participate in communication and is able to alter or modify the information. That's why security during communication scenarios is desired to implement for improving the trustworthiness in network. A large number of security techniques are recently developed for mobile ad hoc network security. But most of the security techniques are emphasized on a specific kind of attack detection and using prevention techniques to remove the effects of attacks. On the other hand the presented study demonstrates the new cryptographic security solution by which a malicious node never joins the network without authenticating .The proposed security model is explained in the further discussion and the simple overview of the proposed system is provided here.

2. LITERATURE SURVEY
In this section the different recent contributions on threshold cryptographic and security issues analysis is provided.

Freshly, there has been interest are developed to obtain effective election processes that has carried as a result of a broad range of applications. Electronic voting protocolis asubstitute to traditional election process. researhers wants to develop advance technique for their applications requirements.Particularlyrequired to design full safety measured to demonstrate a democratic electronic voting system.there are various protocols based on public key are available to provide the safety. In this paper G Gallegos-Garcia et al [22]suggest use of bilinear pairings for security requirements. Therefore electronic voting protocol can be used with public key scheme to enhance security. the developed protocol provides two cryptographic techniques specifically threshold and blind signature based techniques. that are further subdivided in four steps namely setup, authentication, voting and counting. using bilinear pairings this scheme provides seclusion, accuracy and robustness. After design authors provides a comparative analysis based on its performance and key pairs, Trust and Certification Authorities it required.

Internet of things is an developing standard in this model devices (persistent and non-persistent) are connected to each other. The key aim of this connectivity is to provide efficient services related to communication. in this modeling every device are not legitimate in the short time because of an unbounded number of systems, and receipt of their verification request at the similar time. Therefore, protected, and proficient group verification, and authorization scheme is needed that validates a group of devices at once in the context of resource constrained IoTP N. Mahalle et al [23] presents novel Threshold Cryptography-based Group validation (TCGA) scheme for the IoT which confirms authenticity of all the devices taking part in the group communication. This paper also offers TCGA framework which is flexible and safe. The proposed TCGA scheme is executed in the WI-FI environment, and the result demonstrates that TCGA scheme is lightweight, and improves the consequence of battery exhaustion attack. This paper also offers timely analysis, and official security analysis of TCGA scheme which shows that the proposed TCGA scheme is safe from the replay, man-in-the-middle attack, and is scalable in nature.

Classically the key management services are implemented based on Certificate Authority or a Third party Trusted authority. Additionally the previously developed solutions for Mobile ad hoc network security is not much appropriate. MANET features presence a number of challenges such as self-configuring,wireless links, infrastructure less nature. In such conditions Threshold cryptography has proved as effective technique for key management. In this paper N Guptaet earl [24] addresses different approaches for certificate generation, discovery and authentication.

Everywhere calculating is revolutionizing the way humans cooperate with machines and carry out daily tasks. It enlarges daily calculating into the physical world, generating computationallysmart environments that attribute seamless interactions and automation. As a consequence of the extremely distributed nature of ubiquitous calculating, it is important to expand safety mechanisms that lend themselves well to the slight properties of smart ubiquitous calculating environments. In this paper J Al-Muhtadi et al [25] introduce a context-aware access control mechanism that employs threshold cryptography and multilayer encryption to offer a dynamic and really dispersed method for access control. They

simulate access control scheme and show that access control decisions can be made in an appropriate manner even as enhance key and file sizes. This mechanism is directly coupled with the context capturing services and safety policy service resulting in a complete context aware and seamless access control mechanism for distinctive everywhere computing scenarios.

This paper provides an identification technique of compromised nodes.Therefore a determination is made using threshold cryptography and Chinese Remainder Theorem. In this technique each node are assumed as legitimate who concerned in the broadcast process. Then,threshold cryptography is used to share message and Chinese Remainder Theorem is used for routing confirmation. In order to validate is a node is legitimate or not. GSR Emil Selvan et al [26] addresses the issue of compromised nodes.

Key management is a crucial and a determinant security technology to protect wireless and mobile environments such as mobile ad hoc networks (MANETs). Key management problem in MANETshas has been studied in this paper to work out a novel security solution in such dynamic networks. Existing key management schemes for MANETs are chiefly based on certificate-based public key cryptography or identity-based public key cryptography (ID-PKC), which experiences from either the calculated costs of certificates deployment or the key escrow trouble. In this paper, Ze WANG et al [27] present a novel distributed key management scheme, in which a mixture of certificate less public key cryptography (CL-PKC) and threshold cryptography is executed. The proposed scheme attains numerous improved security attributes for key management in MANETs and meanwhile removes the requirement for certificate-based public key distribution and the key escrow trouble efficiently.

Lars Lydersen et al [28] provide a theory named superlinear threshold detector.In this theory a detector has a superior probability to identify photons if it receives them simultaneously rather than at after some time.In quantum key distribution systems superlinear threshold detectors permits eaves-dropping full secret key distribution. Lars Lydersen et al [28] introduces detector control attack and analyze how it executes for key distribution.They compute the superlinearity in superconducting single-photon detectors based on previous published data, and gated avalanche photodiode detectors based on own dimensions. Analysis shows quantum key distribution using detector(s) of either type can be susceptible. The avalanche photodiode detector become superlinear towards the end of the gate. For systems expecting significant loss, or for systems not monitoring loss, this would permit eavesdropping using trigger pulses including less than 120 photons per pulse. Such an attack would be virtually not possible to catch with an optical power meter at the receiver entrance.

In this paper, M. S. A. Mohamad et al [29] propose a threshold authenticated encryption scheme using both factoring and discrete logarithm problems. They apply the concept of threshold cryptography in the verification and message recovery phase, where t out of n recipients are required to verify and recover the message. Security analysis shows that the scheme will remain secure even if one of these problems can be solved.

A large number of little, computationally limited sensor nodes can be linked wirelessly to form a sensor network. Such networks can be utilized to monitor huge areas and communicate a multitude of measurements(such as temperature, humidity, radiation, and so on) to a remote base station. Since this communication occurs over the air interface, the spreaded messages are subject to forgery, manipulation and eavesdropping.Conventional cryptographic countermeasures against these kinds of attacks cannot be eagerly practiced in the context of sensor networks, due to the restricted resources of the individual nodes. Since single nodes can be very simply captured and inspected, symmetric schemes with the covert key there in each (or at least a subset of) node(s) pose quite a threat in this setting. In this work, Manuel Koschuch et al [30] inspect the applicability of threshold cryptographic techniques, particularly the Gennaro-Rabin-Rabin multiparty multiplication protocol, for sensor networks by utilizing various optimizations to the dissimilar steps of this algorithm, building on previous results we attained. They are capable to advance the running time up to a factor of 6 evaluated to a un-optimized version for a bit-length of 1,024 Bit and 33 players.

Biometrics deals with mechanized methods of identifying a person or validating the uniqueness of a person based on the physiological or behavioral characteristic, and so are used for authentication in many of the online transactions. The biometric that has been selected for implementation is fingerprint, since the fingerprint biometric is simply accessible and highly reliable compared to many other biometrics. In the existing biometric validation system the fingerprint template of a person is hired as like in the authentication server and is prone to safety attacks at the server side. To conquer this kind of server side attack, in this paper RajeswariMukeshi et al [31]proposed a system. The fingerprint template is separated into two or more shares using visual cryptographic technique followed by compression. One of these shares is accumulated into the server and the remaining shares are offer to the users. Only these two participants who possess these transparencies can re construct the covert (biometric template) by superimposition of shares.This kind of approach solves two main problems related to fingerprint based regular access control systems such as distortion and expensive preservation of the huge fingerprint database.

3. PROBLEM STATEMENT

Mobile ad hoc network is a promising network technology of future communication networks. A number of researchers are working for improving the communication in such networks. In such networks two areas are major in interest first security and secondly the performance issues. A number of security contributions are placed in recent years, which promising to provide efficient and secure communication. But most of them are less effective in different attack or reducing the performance significantly.

In order to overcome the security issues in network various cryptographic techniques and key exchange mechanism is proposed and implemented in recent years. But due to theoretical and poor design aspects are failing to provide security or compromised with the performance of the network. Thus a secure threshold cryptographic technique is proposed for providing the efficient and secure communication in the network.

The proposed security technique involves the authenticator management, key exchange mechanism and trust computing technique to validate the network routers. This technique evaluates the trust level of each intermediate node in active communication session and prevents that node which is less trustworthy nodes in network. The trust computation depends

on the authenticators which are providing trust values based on the network designers aspect. This section provides overview of the proposed technique and next section involves the detailed understanding of the proposed technique.

4. PROPOSED SOLUTION

4.1 Network configuration

A simple Wi-Fi enabled network devices configured with the proposed routing protocol. The network configuration includes a special kind of network devices known as authenticators. These authenticators are network designer oriented nodes which are randomly chosen from the network nodes. These devices are most trustful devices which are responsible for key generation. A random key is generated by the authenticator node and distributed over the entire network.

4.2 Key generation process

In this phase the routing protocol compute the trust values for all the participating network devices. For that purpose two different trust values namely positive trust and negative trust values are computed. The process of negative and positive trust computation is given as:

$$positive\ trust = c\_1 * SNR + c\_2 * p\_i + c\_3 * E\_i + c\_4 * m\_i$$

Where

$$c_1 + c_2 + c_3 + c_4 = 1$$

And

p_i= packet delivery ratio
E_i =Remaining energy
m_i =Mobility
SNR =Signal to noise ratio

On the other hand the negative trust values are computed using the following formula

$$negative\ trust = 1 - positive\ trust$$

4.3 Key exchange

During the key exchange mechanism the end node (client node) who wants to send data or initiate the communication tries to communicate with the authenticator. Authenticator sends a key to the user. The obtained key is appended to the end user response and send to the target user. Target user extract the appended key from the acknowledge data packet and match with the authenticators key. If the key is matched with two authenticators then the data is accepted otherwise the data is discarded from the node.

4.4 Prevention

The given process helps to identify the trusted nodes on network and the authentic nodes are only premises for communication. Thus after implementing the threshold cryptographic technique is secured and provides the authorized user to communicate.

4.5 Proposed Algorithm

In this section the proposed authentication technique is summarized using algorithm steps for implementation.

1. Initialize the network
2. Select the authenticator
3. Compute trust values (negative trust and positive trust)
4. Generate the session keys
5. Send keys to source devices
6. Append keys to data
7. Send data to target device
8. Evaluate the trust of device
9. If (keys == authenticator key)
10. Node is trusted accept data
11. Else
12. Drop data packets
13. End if

5. RESULTS ANALYSIS

This section provides the detailed discussion about the evaluated results and performance of the propose security algorithm. In addition of that the evaluated parameters are indicating the effect and overheads of the security algorithm.

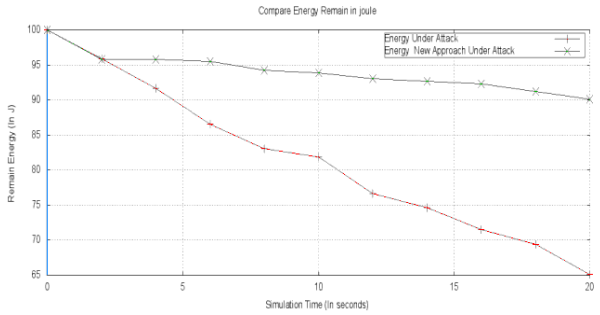

Figure 1: Energy consumption

5.1 Energy

The energy is limited available in ad hoc network devices thus it is an essential parameter for network life time. The amount of energy remaining during communication session is given as the node energy that can be evaluated using the following formula.

Figure 1 shows the energy consumption of network nodes in terms of Jules with the respect of time. Therefore the X axis shows the simulation time of network and the Y axis shows the consumed energy. The performance of network under both the conditions under attack and after prevention of attack is provided using green and red line. According to the obtained results the node consumes their energy rapidly when the network contains a malicious node and the network energy is consumed slowly when the attack is prevented from the attack. Thus the proposed algorithm is functioning as expected and able to prevent the attacker in ad hoc network.

5.2 Routing Overhead

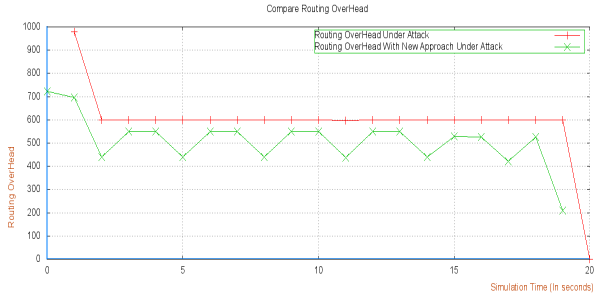

Figure 2: Routing overhead

The routing overhead of network is given using figure 2, the routing overhead indicate the amount of additional data is injected in network during the communication sessions. In the given diagram the X axis demonstrate the simulation time and the respective routing overhead is indicated in Y axis. Additionally, the red line demonstrate the routing overhead under attack conditions and the green line shows the routing

overhead of the proposed routing technique. According to the evaluated results the routing overhead of the proposed technique is much adoptable due to less routing overhead.

5.3 Packet Delivery Ratio

Packet delivery ratio of the proposed technique is given using the figure 3. The amount of successfully delivered data packets are known as the packet delivery ratio. The packet delivery ratio can be computed using the following formula.

Figure 3: P acket Delivery Ratio

According to the given diagram the X axis demonstrate the simulation time in terms of seconds and the Y axis shows the respective packet delivery ratio of network. The packet delivery ratio under attack conditions is given using red line and the green line shows the packet delivery ratio during proposed methodology.

6. CONCLUSIONS

The mobile ad hoc network is a dynamic infrastructure of the communication. In this communication methodology the communicating devices are connected through the wireless links. These wireless links are enabling a user to move within the network randomly in any directions. Thus the route discovery and management is responsibility of the ad hoc network routing protocols. During communication sessions the nodes are first perform the route discovery then the intermediate routers are selected for communication. And if any route is breached then a new path is discovered in network for communication. Thus during this process only once a authentication and trust evaluation can manage the privacy and trust of nodes for communication.

Thus a threshold cryptographic solution is proposed on the proposed work. The proposed technique involves the authenticator management, trust computation and key exchange mechanism for authentic and secure communication. In this technique the authenticators are able to generate the authentication keys and also able to distribute the trust computed keys. These keys are helps to authenticate a user and providing the secure medium for communication. The implementation of the proposed methodology is performed with the help of NS2 (network simulator version 2). Additionally the performance of the system is estimated under different performance parameters. The evaluated outcomes of the proposed authentication technique are summarized using the table 1.

Table 1: Performance Summary

#	Parameters	Description
1	Energy	Able to preserve the energy as compared to the traditional approach of security
2	Routing overhead	Less routing overhead
3	Packet delivery ratio	High packet delivery ratio

According to the evaluated results and the obtained performance of the system, the proposed authentication technique is effective and provides maximum security with less over heads in addition of that acceptable due to the effective performance outcomes.

7. FUTURE WORK

The proposed security system is adoptable and able to serve the secure communication in untrusted environment. This technique is evaluated and designed for DOS detection and prevention of the system. In the near future the proposed work is extended for more attack investigation and improving the end to end delay of network.

8. REFERENCES

[1] H Dey and R Datta, “A Threshold Cryptography Based Authentication Scheme for Mobile Ad-hoc Network”, CCSIT 2011, Part II, CCIS 132, pp. 400–409, 2011 © Springer-Verlag Berlin Heidelberg 2011

[2] S Tarmizi, P Veeraraghavan, S Ghosh, “Extending the Collaboration Boundary in Localized Threshold Cryptography-Based Schemes for MANETs”, Proc. of the 15 -17 Dec, 2009 IEEE 9th Malaysia International Conference on Comm., Kuala Lumpur Malaysia

[3] P Patil, M. A Rizvi, “Improved and Energy Efficient Olsr Protocol Using Spanning Tree in Manet”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 4, Ver. II (Jul-Aug. 2014), PP 38-42

[4] M K Parmar, H B Jethva, “Survey on Mobile ADHOC Network and Security Attacks on Network Layer”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013

[5] Dr. Banta Singh Jangra, Manish Kumar Naga, “Study on Security Issues & Challenges in MANET”, PARIPEX – Indian Journal of Research, Volume : 3 | Issue : 4 | April 2014

[6] Ochola EO, Eloff MM, “A Review of Black Hole Attack on AODV Routing in MANET”, ISSA, 2011 - icsa.cs.up.ac.za

[7] Vikas Solomon Abel, “Survey of Attacks on Mobile Ad hoc Wireless Networks”, (IJCSE) ISSN : 0975-3397 Vol. 3 No. 2 Feb 2011

[8] Animesh Patcha and Amitabh Mishra, “Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks”, 0-7803-7829-6/03/$17.00 0 2003 IEEE

[9] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, licensee Springer. 2011, http://link.springer.com/article/10.1186/2192-1962-1-4/fulltext.html

[10] Shree Om and Mohammad Talib, “Wireless Ad-hoc Network under Black-hole Attack”, 2011 ISSN 2225-658X.

[11] Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil, "Black Hole Attack Injection in Ad hoc Networks".

[12] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Tseng et al. Human-centric Computing and Information Sciences 2011.

[13] Abder Rahmane Baadache, Ali Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks", ISSN 1947-5500 (IJCSIS) Vol. 7, No. 1, 2010.

[14] Varsha Patidar, Rakesh Verma, "Black Hole Attack and its Counter Measures in AODV Routing Protocol", ISSN 2250-3005 Sep. 2012

[15] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[16] Nishant Sitapara, Sandeep B. Vanjale, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks, ICETE-201O" on Emerging trends in engineering on 21st Feb 2010.

[17] Kamatchi.V1, Rajeswari Mukesh2,Rajakumar3, "Black Hole Attack Prevention Using random Dispersive Routing For mobile ad hoc Networks", (Ijans) Vol. 2, No. 4, October 2012.

[18] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, Abbas Jamalipour, "A survey of routing attacks in mobile ad hoc networks", 1536-1284/07/$20.00 © 2007 ieee.

[19] S. A. Ade & P. A. Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks", International Journal of Information Technology and Knowledge Management, July-Dec 2010, Volume 2, No. 2, pp. 545-548

[20] Vinay Sridhara, Nagendra Subramanya, "Evaluating Different Techniques to Improve TCP Performance over Wireless Ad Hoc Networks", http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.80.8842

[21] M. S. karthikeyan, K. Angayarkanni, and Dr. S. Sujatha, "Throughput Enhancement in Scalable MANETs using Proactive and Reactive Routing Protocols", proceedings of the international multi conference of engineering and computer scientists, Vol II, march 2010.

[22] G Gallegos-Garcia, R Gomez-Cardenas, Gonzalo I. D-Sanchez, "Identity based Threshold Cryptography and Blind Signatures for Electronic Voting", WSEAS Transactions on Computer, Issue 1, Volume 9, January 2010

[23] P N. Mahalle, N R Prasad and R Prasad, "Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)", Published in: IEEE ANTS 2013 Seventh IEEE International Conference on Advanced Networks and Telecommunication Systems (ANTS)

[24] N Gupta, M Shrivastava, A Goel, "Survey paper on different approaches of Threshold Cryptography", International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970), Volume-2 Number-3 Issue-5 September-2012

[25] J Al-Muhtadi, R Hill, S Al-Rwais, "Access control using threshold cryptography for ubiquitous computing environments", Journal of King Saud University – Computer and Information Sciences (2011) 23, 71–78

[26] GSR Emil Selvan, Dr. M. Suganthi, P Jeni, KA Krishna Priya, "Detection of Compromised Nodes in Mobile Ad-Hoc Networks", Journal of Computational Information Systems 7: 6 (2011) 1823-1829

[27] Ze WANG, Lu LI, Jigang WU, Wei ZOU, "An Efficient Certificateless Key Management Scheme in Mobile Ad Hoc Networks", Journal of Computational Information Systems 9: 12 (2013) 4787–4794

[28] Lars Lydersen, Nitin Jain, Christoffer Wittmann, ystein Marøy, Johannes Skaar, Christoph Marquardt, Vadim Makarov, and Gerd Leuchs, "Super linear threshold detectors in quantum cryptography", arXiv:1106.2119v2 [quant-ph] 17 Aug 2011

[29] M. S. A. Mohamad, E. S. Ismail, "A Threshold Authenticated Encryption Scheme Using Hybrid Problems", Applied Mathematical Sciences, Vol. 8, 2014, no. 31, 1499 – 1507, HIKARI Ltd, www.m-hikari.com, http://dx.doi.org/10.12988/ams.2014.4142

[30] Manuel Koschuch, Matthias Hudler, Michael Kruger, Peter Lory, Jurgen Wenzl, "Optimizing Cryptographic Threshold Schemes For The Use In Wireless Sensor Networks", DCNET 2011 Position Paper

[31] Rajeswari Mukeshi, V.J.Subashini, "Fingerprint Based Authentication System Using Threshold Visual Cryptographic Technique", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012