Mutual authenticated key agreement in Wireless Infrastructure-less network by Chaotic Maps based Diffie-Helman Property

D. Neela M. Shyam*, Mohammed Ali Hussain

Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram Guntur Dist., A.P., India
Emails: n.m.s.desai@hotmail.com; dralihussain@kluniversity.in

Abstract

Because wireless infrastructure-less networks are dynamic, varied, and scattered, implementing security in them is exceedingly difficult. Authentication is the most crucial prerequisite for security deployment. It is difficult to implement security based on public-key infrastructure with centralized third-party authentication in an environment without infrastructure. We build and test a chaotic map-based technique that handles authentication as one of the key qualities to accomplish security. We allocate the key management responsibility to cluster-heads after dividing the infrastructure-less into several clusters with cluster-heads. The Diffie-Helman property, which is based on Chebyshev polynomials, is used in the proposed work to establish authentication. Our suggested method avoids unnecessary computations like modular exponentiation and elliptical curve scalar multiplications. It also ensures that the secret session-key is only established between the two designated entities and is resistant to a variety of network attacks.

Keywords: Wireless Infra structure less networks; authenticated key agreement; clusters; Diffie-Helman Property; attacks.

1. Introduction

In our daily lives, the use of computers and their connectivity have become essential. In the past, wired networks were used to connect computers and were adequate for a long time. Later, the demand for wireless networks was very great. Wireless local area networks built on IEEE 802.11 specifications were responsible for achieving it. Nevertheless, developing wireless communication systems with autonomous mobile users is necessary for the next generation. These networks are essential for military operations, conferencing, online learning, risk management, disaster recovery, and emergency services. Wireless Infrastructure-less networks can be used to fill this demand [1,2,3].

Wireless communication networks of the first generation used analog technology. With AMPS innovation, its primary goal was to allow voice and data connectivity at low data rates. It offered a 10-kbps data rate on 832 channels of the 40 kHz spectrum. Following this, wireless communications underwent a lot of innovation. Multimedia transmission with quality-of-service support and mobile broadband features were introduced. Second generation systems, such as GSM, cordless phones, DECT, and PACS, are based on digital multiple-access skills like (CDMA and TDMA), with GSM using the TDMA method. Then, the GPRS idea, based on radio skills, was presented. This was the 2.5 generation, or 2.5G, in which the GSM network was used to implement packet switching. To have adjustable data speed and continuous network connectivity, packets were divided into small chunks in this system. The 3G evolution is so-called [9].

Later, DARPA research presented the idea of an infrastructure-less network. On the battlefield, numerous wireless nodes use packet-switching technology to communicate with one another in a system known as a packet radio network (PRNET). It introduced multiple-hop ALOHA communication via extensions with an extended range. ALOHA developed the idea of using the radio signals' broadcasting properties to transmit and retrieve data packets in a single communication hop. The PRNET was technically capable of initiating and organizing itself. It indicates that even without a base station, a network's nodes may organize themselves and establish radio communication.

Doi: https://doi.org/10.54216/FPA.130211
Received: April 10, 2023 Revised: July 22, 2023 Accepted: October 05, 2023

Due to its peer-to-peer networking, lack of infrastructure, and scattered nature, PRNET differed significantly from wired networks. These characteristics contributed to the development of wireless Infrastructure-less networks.

The purpose of wireless Infrastructure-less networks is always to support the network in all places. The network lack infrastructure and is independently configured and maintained. It is a wireless network made up of various mobile nodes (devices) that are linked together to create a topology that changes dynamically. It lacks a base station, fixed infrastructure, or central coordinator to manage network communication. Each node has the network-intelligence to function as both a host and a router. To put it another way, the networks function as peer-to-peer networks. The nodes can operate independently and are interconnected via several links and heterogeneous radio transmission. These qualities make networks ideally suited for situations when setting up the network infrastructure is complicated, and the network is time as well as cost efficient.

Due to distributed, dynamic, peer-to-peer, and heterogeneous characteristics of wireless Infrastructure-less networks, security deployment is complicated. Additionally, there is no obvious line of protection when developing security. Limitations on battery, buffer, and node computation make Infrastructure-less networks susceptible to security solution development. Therefore, security mechanisms are needed for networks that guarantee both securities and consider their constrained resources. Mutual authenticated-key agreement is a straightforward and practical prerequisite for deploying security. It is a technique wherein two designated entities in a network authenticate and share a secret key based on the data they have both provided. The mutual authentication and key agreement ensure that the secret session-key is only formed between the two designated entities. It is essential to prevent unauthorized entities from entering the network environment. Because the nodes in wireless Infrastructure-less networks are autonomous, they may demonstrate and confirm their legitimacy without needing an outside authority. Hence it is relevant to Infrastructure-less networks.

Cryptographic operations consume resources in terms of battery, buffer, and processor. Therefore, reducing resource consumption during cryptographic operations is the most crucial factor to consider while developing a security mechanism for wireless Infrastructure-less networks. In this network's context, the primary objective of the security protocol is not merely to offer authentication and authorization but also to focus on network longevity. Resource conservation and security are, therefore, the most important factors to consider when creating a security mechanism for this network.The primary goal in a resource-constrained environment is to provide security while maximizing resource efficiency [7]. Many security schemes and resource efficiency strategies are put out for the infrastructure-less network environment. Sadly, none of these strategies are well suited for Infrastructure-less network applications, such as on the battlefield. Therefore, a single method that combines security and resource efficiency is highly desirable. To accomplish this, we describe a technique named "Mutual authenticated key agreement in Wireless Infrastructure-less network by Chaotic Maps based Diffie-Helman Property." The proposed method provides security using Chebyshev polynomials and avoids unnecessary computations like modular exponentiation and elliptical curve scalar multiplications to deliver resource efficiency.

1.1. Security in Wireless Infrastructure-less network

Due to the dynamic network architecture, limited resources, inaccurate state information, lack of centralized coordination, hidden and exposed node problems, and wireless infrastructure-less networks, implementing security is a difficult challenge. There is no absolute line of defense for building security, and there is no clearly defined spot to implement a security explanation. Each node in an infrastructure-less network works as a host and router, i.e., it functions as a peer-to-peer network. The vulnerability of infrastructure-less networks is caused by the physical capture of heterogeneous nodes. Due to limited processing capability, hackers may use these subverted nodes to enter the network and execute demanding tasks like cryptographic calculation.

Link layer protocols provide single-hop communication in infrastructure-less networks, while network layer protocols enable multi-hop communication. Both protocols make the premise that mobile nodes in a network cooperate and collaborate the communication. However, this assumption is false in hostile environments. In infrastructure-less networks, cooperation is expected but not required. By disregarding the protocol requirements, malicious attackers can easily disrupt network operations. Routing and packet forwarding are two tasks performed by the network layer. However, both are susceptible to malicious activity, which can result in different kinds of network layer attacks. The most crucial requirement for deploying security in any network environment is "authentication." The security potency of any authentication mechanism depends on its key-management method. Numerous secure protocols based on key management in infrastructure-less networks have been proposed in the literature. These protocols were primarily divided into two categories.

- Centralized key management mechanisms [10]
- Distributed key management mechanisms [11]

Doi: https://doi.org/10.54216/FPA.130211
Received: April 10, 2023 Revised: July 22, 2023 Accepted: October 05, 2023

Distributed mechanisms based on the Group "Diffie-Hellman Key" method generate a random number between two targeted nodes so that an intruder has no chance of knowing it. Multiple public key operations add overhead to these protocols, making them unsuitable for time-sensitive applications. 'Key pre-distribution (KPS) is the basis for centralized key distribution protocols. Before group communication, these mechanisms rely on a trusted third-party to communicate sensitive information with other network nodes. As a result, confidential users can generate specific keys and contribute to communication [12-16].

Mechanisms that are centrally managed have a single point of collapse. Shared key mechanisms for distributed key management assume that network nodes are trustworthy and behave appropriately. However, this presumption is incorrect in the context of infrastructure-less networks. Numerous cryptographic methods, including hashing, symmetric key encryption, and asymmetric key encryption, have been created since the introduction of chaos theory to cryptography. To boost security while needing less overhead, chaos-based key agreement mechanisms, such as two-party and multi-party key agreements mechanisms, have been created. None of these protocols, however, made any effort to be resource efficient. To deal with the dynamic scattered network topology of infrastructure-less networks, our work's primary purpose is to establish secure communication with security aim authentication and further effective resource deployment. We partition the network into several classes based on previous work CGSR. Every group consists of a cluster-head (CH), a cluster member (CM), and a gateway (GW). The CH oversees cluster organization, while the GW oversees inter-cluster communication. Our work expands the CGSR, incorporating security features and a resource-saving idea. The capacity of a node to process optimal data packets is the basis for choosing the cluster-head. It is determined using the node's remaining energy and current traffic; we used the existing work [4] to select the cluster-head. Every node in a network settles on public key pairs for end-to-end encryption and uses Chebyshev polynomials to create a secure session-key. The composition property of a Chebyshev-polynomial introduces the idea of a two-entity key agreement, which enables two interacting entities to share a secured key by exchanging their public keys across an unsecured channel [17-18].

1.2. Mutual authenticated key agreement

1.2.1. Cluster Formation

The process of clustering involves breaking up a network into several interconnected subclusters. By delivering services locally, clustering in a network can increase the availability of network resources, solve the scalability problem, avoid expensive long-distance communication, and provide a better solution for the key management issue. A cluster-head is present in every cluster for coordinating purposes. In the network model for the proposed system, mobile nodes are grouped into several clusters so that every node is included in the clustering process, and none is left out. Additionally, one node from each cluster is selected as the cluster-head, responsible for carrying out the administration, key management, and coordinating tasks for the cluster. As clustering integrates both distributed and centralized methods, it also reduces the several keys required for secure communication. It enables efficient key management, our approach's primary goal of clustering.

Successful clustering separates the network into several groups while long-term maintaining the network's structure. The choice of the cluster-head is essential since a failed cluster-head might lead to the collapse of the cluster. The cluster-head oversees organizing the cluster and must be in a better resource-related state in the cluster-based network architecture. To choose the cluster-head, we calculated the node's optimum data packet processing capacity (ODPPC). Every node in a network must perform the algorithm proposed in [6] whenever one is created to determine its " ODPPC " values. We are defining a threshold value, ODPPCMAX, which is the value determined by the node under ideal circumstances, such as when the battery is fully charged, and there is little traffic in the inline buffer queue. When nodes with reduced mobility have optimal packet processing capacities larger than ODPPCMAX, they serve as the cluster-head. The rest of the network construction is identical to the current "CHGSR" [4].

2. Cluster-Based Mutual Authentication

Conventional public key architectures include a fixed registration center (RC), and network participants use this protected data to communicate and establish identities with one another. System security is compromised since it relies intensely on a single node and has a single point of failure. Due to their distributed behavior, infrastructure-less networks demand a distributed authentication strategy. The registration center is shared among the cluster-heads in the architecture for our designed Cluster Based Mutual Authentication and key Settlement, and any cluster-head may function as an RC. It is a solution to the single-point security issue. By using Chebyshev-polynomials, which are described as follows [8];

$$T_{n+1}(X) = 2 * T_n(X) - T_{n-1}(X) \text{ , } n \geq 1 \qquad \ldots\ldots\ldots\ldots\ldots 1$$

Doi: https://doi.org/10.54216/FPA.130211
Received: April 10, 2023 Revised: July 22, 2023 Accepted: October 05, 2023

The Chebyshev-polynomial $T_n(X)$, which has a degree of n, is represented by equation 1. The following leverages the semi-group property of Chebyshev-polynomials to offer authentication.

$$T_n(X) = (2 * T_{n-1}(X) - T_{n-2}(X)) * (\text{mod } N),\ n \geq 2 \quad \ldots\ldots\ldots\ldots\ldots\ldots 2$$

N is a large prime number and $X \epsilon (-\infty, +\infty)$. Finding the value of 'n' in equation (2) given $T_n(X)$, N and X are theoretically impossible, i.e., Chaotic Maps-Based Discrete Logarithm Problem. According to Chebyshev, polynomials' composition property is given in equation (3)

$$T_m(T_n(X)) = T_m(T_n(X)) = T_{mn}(X), \quad m \geq 0 \ \& \ n \geq 0 \quad \ldots\ldots\ldots\ldots 3$$

Finding the value of $T_{mn}(X)$ in equation (3), given $T_n(X)$, $T_m(X)$, X and N is theoretically impossible, i.e., Chaotic Maps Based Diffie-Hellman problem. The proposed authentication algorithm uses both the properties mentioned in equations 2 and 3.

2.1. Key Generation and Distribution

Chebyshev polynomials-based cluster authentication architecture is the foundation of our work. Consider an infrastructure-less network with clusters, each with a cluster-head CH_i with $(i = 1,2,3 \ldots.)$ and cluster members $CM_i (i = 1,2,3 \ldots.)$. The following consideration is made regarding the proposed algorithm.

In infrastructure-less networks, each node is assigned a distinct identity, such as a cluster-head ID_{CH_i} with $(i = 1,2,3 \ldots.)$ and cluster members ID_{CM_i} $(i = 1,2,3 \ldots.)$. We assume that a reliable offline outside party will choose the network's symmetric cryptosystem and trusted one-way hash function. All cluster-heads in a network to choose large prime numbers PNH and private key K_{prh} at random and compute the values of $T_{K_{prh}}(PNH)$ From equation (2), here public information is an identity of the cluster, prime number, and $T_{K_{prh}}(PNH)$. The private information is K_{prh}.

All cluster members in a network to choose large prime numbers PNM and private key K_{prm} at random and compute the values of $T_{K_{prm}}(PNM)$ from equation (2), here public information is the identity of the cluster, prime number, and $T_{K_{prm}}(PNM)$. The private information is K_{prm}. When a cluster forms, whenever new updates take place, and whenever a new cluster member joins, the cluster-head makes public information available to all cluster members.

Whenever a cluster member becomes a source, or the cluster-head makes a request, public information about the cluster member is sent to the cluster-head.

Our authentication method uses two keys, a Cluster-key and a Session-key, to enable strong authentication. Whenever a new node joins the cluster, and the cluster-head is informed via a hello message. Identities, the cluster-head's public key, and standard encryption and decryption procedures are among the public information that the cluster-head communicates to cluster members. With the help of the cluster-head's public key, the node will calculate the cluster key and provide the cluster-head with its public key. Authentication between cluster members and the cluster-head is done via the cluster key. The cluster-head and each node must agree upon a cluster key. Node exits the cluster and joins another cluster as a result of mobility. The enrolling node is treated as a new node by the new cluster-head, and as a result, the node and cluster-head concur on the cluster key depicted in Figure 1. After a predetermined amount of time, the old cluster deletes the entry and associated cluster key of the relocated node. Cluster keys act as authentication since they are used to compute and share the session-key between two communicating nodes. The entire communication must be encrypted and decrypted using the session-key to guarantee complete information secrecy.

2.2. Algorithm

Consider a cluster-based infrastructure-less network with cluster-head 'CH' and several cluster members. Consider two cluster members CMA and CHB want to authenticate each other. The public information about the cluster is, $\left\{PN, ID_{CH}, ID_{CMA}, ID_{CMB}, T_{K_{prh}}(PN)\right\}$, Hash function, symmetric encipherment.

Step1: Cluster member CMA selects the Private key K_{prcma} and calculate the value of $T_{K_{prcma}}(PN)$ and $K_{CH-CMA} = T_{K_{prcma}} T_{K_{prh}}(PN)$ with the help of public information.

Then CMA constructs the message m_{CMA} as follows

Doi: https://doi.org/10.54216/FPA.130211
Received: April 10, 2023 Revised: July 22, 2023 Accepted: October 05, 2023

$$m_{CMA} = \left\{ID_{CMA}, ID_{CMB}, ID_{CH}, T_{K_{prcma}}(PN), CT_{CMA}\right\}$$

Where,

$$CT_{CMA} = E\left(K_{CH-CMA}, \quad \left\{ID_{CMA}||ID_{CMB}||ID_{CH}||H_{CMA}\right\}\right)$$

$$H_{CMA} = \left\{ID_{CMA}||ID_{CMB}||ID_{CH}||T_{K_{prcma}}(PN)\right\}$$

Cluster member CMA sends the m_{CMA} to 'CH, and this message indicates that it wants to authenticate with Cluster member CMB

Step 2: After reception of the message $m_{CMA}$from the cluster member, the cluster-head computes the key $K_{CMA-CH} = T_{K_{prh}} T_{K_{prcma}}(PN)$ using the value $T_{K_{prcma}}(PN)$ which is received from m_{CMA}. Then it decrypts the CT_{CMA} using key K_{CMA-CH}, and further, validate the message by computing the hash value H_{CMA}. Then cluster-head sends the message m_{CH} to cluster member CMB to indicate that CMA wants to authenticate with you.

$$m_{CH} = \left\{ID_{CMA}, ID_{CMB}, ID_{CH}, T_{K_{prh}}(PN)\right\}$$

Step 3: Cluster member CMB selects the Private key K_{prcmb} and calculate the value of $T_{K_{prcmb}}(PN)$ and $K_{CH-CMB} = T_{K_{prcmb}} T_{K_{prh}}(PN)$ with the help of public information.

Then CMB constructs the message m_{CMB} as follows

$$m_{CMB} = \left\{ID_{CMA}, ID_{CMB}, ID_{CH}, T_{K_{prcmb}}(PN), CT_{CMB}\right\}$$

Where,

$$CT_{CMB} = E\left(K_{CH-CMB}, \quad \left\{ID_{CMA}||ID_{CMB}||ID_{CH}||H_{CMB}\right\}\right)$$

$$H_{CMB} = \left\{ID_{CMA}||ID_{CMB}||ID_{CH}||T_{K_{prcmb}}(PN)\right\}$$

Cluster member CMB sends the m_{CMB} to 'CH, and this message indicates that it wants to authenticate with Cluster member CMA

Step 4: After reception of the message $m_{CMB}$from the cluster member, the cluster-head computes the key $K_{CMB-CH} = T_{K_{prh}} T_{K_{prcmb}}(PN)$ using the value $T_{K_{prcmb}}(PN)$ which is received from m_{CMB}. Then it decrypts the CT_{CMB} using key K_{CMB-CH}, and further, validate the message by computing the hash value H_{CMB}. Further, the Cluster-head computes the session-key $K_{A-B} = T_{K_{prcma}} T_{K_{prcmb}}(PN)$ with the received information from CMA and CMB through messages m_{CMA} and m_{CMB} respectively.

Step 5: Using their lengthy secret keys, the cluster-head encrypts and securely transmits the session-key to nodes CMA and CMB.

$$m_{CMA-SK=E(K_{CH-CMA}, K_{A-B})}$$

$$m_{CMB-SK=E(K_{CH-CMB}, K_{A-B})}$$

Step 6:

Using their lengthy secret keys, Nodes CMA and CMB., respectively, decrypt the messages m_{CMA-SK} and m_{CMB-SK} to obtain the session-key K_{A-B}. Right now, every message is encrypted with a session-key between CMA and CMB. Figure -1 shows the mutual authentication flowchart.

Mutual authentication mechanism flowchart

Doi: https://doi.org/10.54216/FPA.130211
Received: April 10, 2023 Revised: July 22, 2023 Accepted: October 05, 2023

Select large prime numbers PNM and private key K_{prm} at random and compute the values of $T_{K_{prm}}(PNM)$

large prime numbers PNH and private key K_{prh} at random and compute the values of $T_{K_{prh}}(PNH)$

Select large prime numbers PNM and private key K_{prm} at random and compute the values of $T_{K_{prm}}(PNM)$

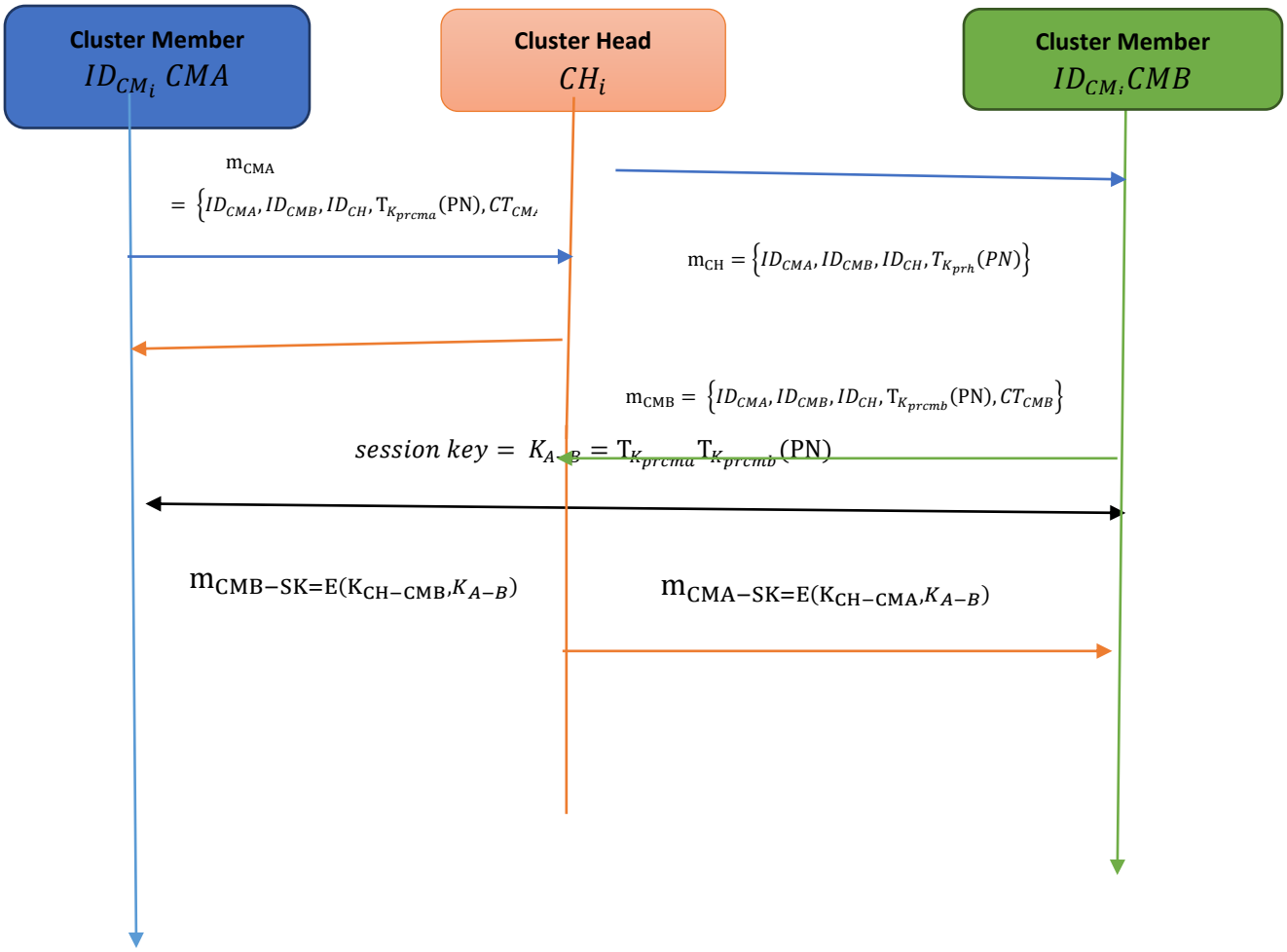

Figure 1: flow chart of the mutual authentication mechanism

3. Performance Calculations

One of the cryptographic mechanisms, which employed with public-key infrastructure is based on chaotic maps; the other mechanisms are based on discrete logarithms, elliptic curves, and integer factorizations. The Digital Signature methods are the best examples of discrete logarithms, while a good example of an integer factorization mechanism is the RSA cryptography system. Elliptic curve cryptography techniques are more effective than RSA for wireless network environments since they are based on elliptic curves. ECC offers a smaller key, faster computation, and identical security "reference" in contrast to RSA. Chebyshev polynomial computing provides smaller key sizes, speedier computation, and resource savings than ECC and RSA.

Paper compares the proposed work with existing ECC Based key-agreement mechanism for infrastructure-less networks [5]. It is developed for authenticating two communicating entities and key agreement. The existing provided the comprehensive assessment with the other four key-agreement mechanisms about computational overhead, showing that the proposed model is adequate. As a result, in this section, we merely contrast our plan with the existing mechanism. Power consumption is a constant concern and is difficult to quantify in infrastructure-less networks since it is a heterogeneous network with limited resources. As a result, we assessed the calculation costs for performance evaluation at participating nodes in key agreement using the primitive operation count. The cost calculation notation is as follows:

Doi: https://doi.org/10.54216/FPA.130211
Received: April 10, 2023 Revised: July 22, 2023 Accepted: October 05, 2023

1. T_{Cheb} stands for the computation time for the Chebyshev polynomial.

2. T_{ECC} stands for the elliptic curve point multiplication execution time.

Chebyshev-polynomial computation presents a smaller key size, speedier calculation, and resource savings as compared to ECC and RSA. Additionally, ECC provides computing overhead through modular exponentiation and scalar multiplication. According to Hongfeng Zhu, in an identical resource and network environment, the Chebyshev polynomial operation (Tcheb) executes 0.042055 s quicker than the elliptic curve point-multiplication (TEcc) operation.

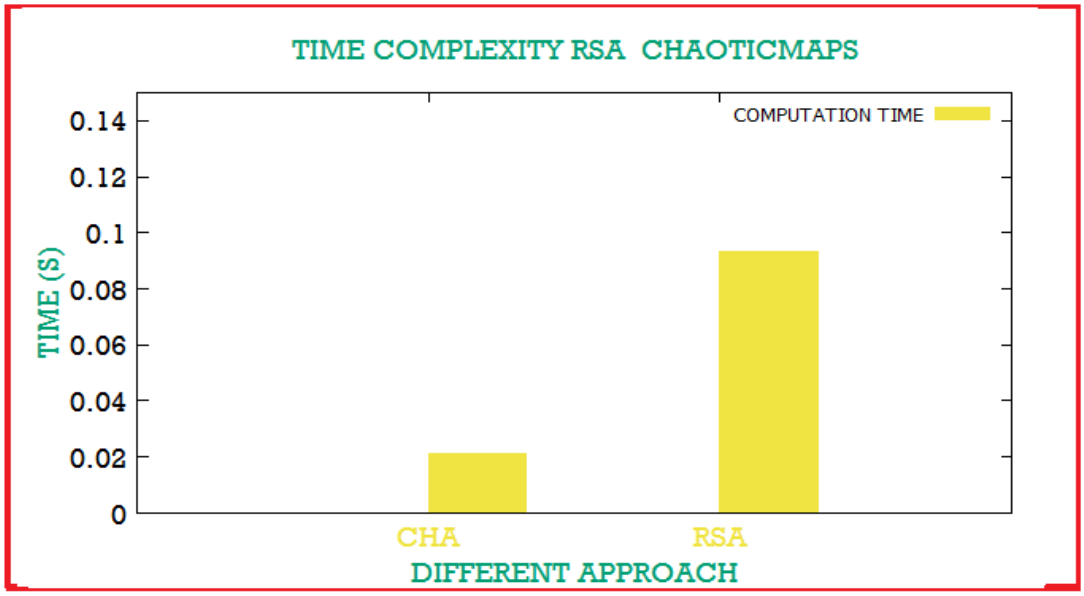

Figure 2: Comparison between RSA and Chaotic Maps in computational time.

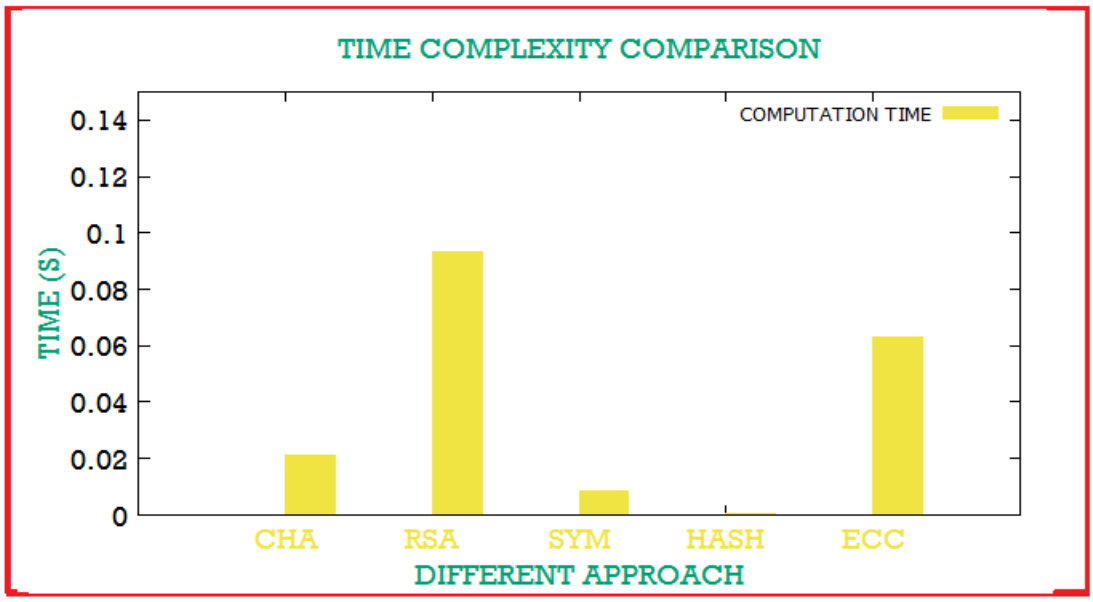

Figure 3: Comparison between RSA, ECC and Chaotic Maps in computational time.

In our comprehensive evaluation of cryptographic algorithms within a standardized computational environment comprising a dual-core 2.33 GHz processor, 2 GB DDR2 RAM, and 160 GB Hard Disk Capacity, we conducted a thorough analysis by varying prime number sizes up to 1024 bits in length. The primary focus of our investigation was to assess the computational performance of two prominent encryption methods: RSA (Rivest–Shamir–Adleman) and Chaotic Maps. Our findings revealed a significant divergence in computational efficiency between

Doi: https://doi.org/10.54216/FPA.130211
Received: April 10, 2023 Revised: July 22, 2023 Accepted: October 05, 2023

these two approaches, as illustrated in Figure 1. Notably, Chaotic Maps exhibited substantially longer computational times in comparison to RSA and ECC (Elliptic Curve Cryptography), as demonstrated in Figure 2. This outcome underscores the computational capacity limitations of Chaotic Maps in the context of our specific environment. Furthermore, we emphasize that computational time directly impacts network performance metrics, including end-to-end delays, energy consumption, and buffer space utilization, all of which are vital considerations for secure and efficient data transmission in networked system.

3.1. Security Evaluation

Security evaluation of the designed mechanism is as follows,

To calculate the cluster key and session key—both of which cannot be solved in polynomial time, as we utilized the security factor based on the chaotic maps-based Diffie-Hellman and discrete logarithm problems.

Considering the attacker has complete command to access the network and use an unsecured channel to carry out destructive actions. The attacker cannot obtain the knowledge necessary to calculate the cluster and session-keys, though. Our key generation technique offers lower key sizes, faster computation, less memory usage, and energy consumption than key generation algorithms like RSA and ECC, making it ideally suited for infrastructure-less networks.

Since the session-key is created proactively rather than passively and no data is saved on the network, our architecture is resistant to both modification and stolen verification attacks. Because nodes can modify and revise the cluster key, our mechanism is resistant to guessing attacks. To assess the security strength of our proposed protocol, we implemented it within the AVISPA tool, which, in turn, executed the algorithm. The results of this evaluation are depicted in Figure 3, providing valuable insights into the security attributes and robustness of our protocol design. This formal analysis is instrumental in ensuring that our protocol meets the stringent security requirements essential for its intended application.

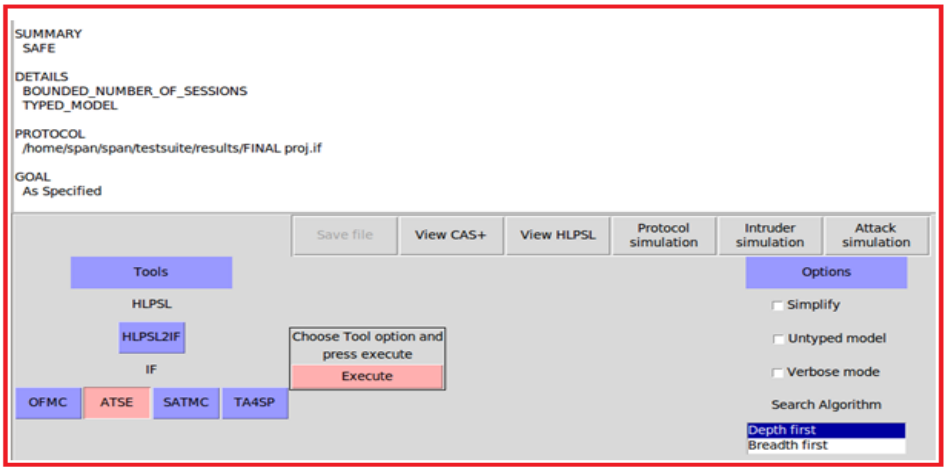

Figure 4: Simulation Result of Mutual Authentication Algorithm

4. Conclusion

Because wireless infrastructure-less networks are dynamic, varied, and scattered, implementing security in them is exceedingly difficult. Authentication is the most crucial prerequisite for security deployment. It is difficult to implement security by public-key infrastructure with centralized third-party authentication in an environment without infrastructure. We build and test a chaotic map-based technique that handles authentication as one of the key qualities to accomplish security. We allocate the key management responsibility to cluster-heads after dividing the infrastructure-less into several clusters with cluster-heads. The Diffie-Helman property, which is based on Chebyshev polynomials, is used in the proposed work to establish authentication. Our developed method avoids unnecessary computations like modular exponentiation and elliptical curve scalar multiplications. It also ensured that the secret session-key is only established between the two designated entities and is resistance to a variety of network attacks.

Doi: https://doi.org/10.54216/FPA.130211
Received: April 10, 2023 Revised: July 22, 2023 Accepted: October 05, 2023

References

[1] Bang, Ankur O., and Prabhakar L. Ramteke. "MANET: History, challenges and applications." International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2.9 (2013): 249-251.

[2] Raja, L., and S. Santhosh Baboo. "An overview of MANET: Applications, attacks and challenges." International journal of computer science and mobile computing 3.1 (2014): 408-417.

[3] Chitkara, Mahima, and Mohd Waseem Ahmad. "Review on manet: characteristics, challenges, imperatives and routing protocols." International journal of computer science and mobile computing 3.2 (2014): 432-437.

[4] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks." Indian Journal of Science and Technology 9 (2016): 26.

[5] Yadav, Dega Ravi Kumar, K. Nikitha Reddy, and N. Vamshi Krishna. "Authenticated Mutual Communication between two Nodes in MANETs." International Journal of Computer Science and Information Technologies 4.2 (2013): 331-333.

[6] Mohammad, Arshad Ahmad Khan, Ali Mirza Mahmood, and Srikanth Vemuru. "Energy-Aware Reliable Routing by Considering Current Residual Condition of Nodes in MANETs." Soft Computing in Data Analytics. Springer, Singapore, 2019. 441-452.

[7] Mohammad, Arshad Ahmad Khan, Ali Mirza Mahmood, and Srikanth Vemuru. "Intentional and unintentional misbehaving node detection and prevention in mobile ad hoc network." International Journal of Hybrid Intelligence 1.2-3 (2019): 239-267.

[8] Mason, John C., and David C. Handscomb. Chebyshev polynomials. Chapman and Hall/CRC, 2002.

[9] Tse, David, and Pramod Viswanath. Fundamentals of wireless communication. Cambridge university press, 2005.

[10] Rafaeli, Sandro, and David Hutchison. "A survey of key management for secure group communication." ACM Computing Surveys (CSUR) 35.3 (2003): 309-329.

[11] He, Xiaobing, Michael Niedermeier, and Hermann De Meer. "Dynamic key management in wireless sensor networks: A survey." Journal of network and computer applications 36.2 (2013): 611-622.

[12] A. Irshad, M. Sher, S. A. Chaudhry, H. Naqvi, and M. S. Farash, "An efficient and anonymous multi-server authenticated key agreement based on chaotic map without engaging Registration Centre," The Journal of Supercomputing, vol. 72, pp. 1623–1644, Mar. 2016. [Online]. Available: https://link.springer.com/article/10.1007/s11227-016-1688-9.

[13] J. Li, X. Niu, and W. Sun, "Security analysis and improvement of a mutual authentication and key agreement solution for wireless sensor networks using chaotic maps," International Journal of Distributed Sensor Networks, vol. 11, no. 3, p. 793592, Mar. 2015. [Online]. Available: https://journals.sagepub.com/doi/10.1155/2015/793592.

[14] A. Irshad, M. Sher, S. A. Chaudhry, H. Naqvi, and M. S. Farash, "An efficient and anonymous multi-server authenticated key agreement based on chaotic map without engaging Registration Centre," The Journal of Supercomputing, vol. 72, pp. 1623–1644, Mar. 2016. [Online]. Available: https://link.springer.com/article/10.1007/s11227-016-1688-9

[15] J. Li, X. Niu, and W. Sun, "Security analysis and improvement of a mutual authentication and key agreement solution for wireless sensor networks using chaotic maps," International Journal of Distributed Sensor Networks, vol. 11, no. 3, p. 793592, Mar. 2015. [Online]. Available: https://journals.sagepub.com/doi/10.1155/2015/793592

[16] A. Irshad, M. Sher, S. A. Chaudhry, H. Naqvi, and M. S. Farash, "An efficient and anonymous multi-server authenticated key agreement based on chaotic map without engaging Registration Centre," The Journal of Supercomputing, vol. 72, pp. 1623–1644, Mar. 2016. [Online]. Available: https://link.springer.com/article/10.1007/s11227-016-1688-9

[17] Balakrishnan, C.; Ambeth Kumar, V.D. IoT-Enabled Classification of Echocardiogram Images for Cardiovascular Disease Risk Prediction with Pre-Trained Recurrent Convolutional Neural Networks. Diagnostics 2023, 13, 775. https://doi.org/10.3390/diagnostics13040775

[18] Sathya Preiya, V.; Kumar, V.D.A. Deep Learning-Based Classification and Feature Extraction for Predicting Pathogenesis of Foot Ulcers in Patients with Diabetes. Diagnostics 2023, 13, 1983. https://doi.org/10.3390/diagnostics13121983

Doi: https://doi.org/10.54216/FPA.130211
Received: April 10, 2023 Revised: July 22, 2023 Accepted: October 05, 2023