A NOVEL EXTENSIBLE AUTHENTICATION PROTOCOL BASED GROUP AUTHENTICATION AND KEY AGREEMENT PROTOCOL FOR WIRELESS NETWORKING

Pranth.M¹ | P.Sangeetha²

¹(Department of Computer science, Tamilnadu College of Engineering, Coimbatore.)
²(Department of Computer science, Assistant Professor, Tamilnadu College of Engineering, Coimbatore.)

Abstract—By utilizing the broadcast nature of radio channels, cooperative wireless communications exploits a brand new degree of freedom to combat unfavorable wireless channel conditions with the help of relays. The transmission reliability and rates achieved by cooperation for various communication eventualities and cooperation schemes are extensively studied. However, additionally to the benefits it brings to wireless networking, cooperation additionally raises some sensible problems, among that data security is maybe the foremost vital. During this work propose a gagle authentication and key agreement protocol, known as EG-AKA, for wireless networking communications combining elliptic curve Diffie-Hellman (ECDH) supported EAP framework. Compared with typical EAP-AKA, the planned protocol guarantees stronger security and provides higher performance. Elaborated security analysis has shown that the planned EG-AKA protocol is secure in terms of user and cluster identity protection and resistance to many attacks. Moreover, the planned protocol is secure against numerous malicious attacks through the performance analysis and its potency is just too high in terms of the sign overhead, the bandwidth consumption, and also the transmission price.

Keywords— Elliptic Curve Diffie-Hellman, Wireless Networking, Extensible Authentication Protocol, Group Authentication and Key Agreement Protocol

1. INTRODUCTION

An elementary downside of all wireless communications is that the secure distribution of secret keys, that should be generated and shared between licensed parties before the beginning of communication. Within the field of cryptography, the Diffie-Hellman key exchange protocol is one in all the foremost basic and wide used cryptanalytic protocols for secure key institution. The essential plan behind the Diffie-Hellma n key exchange is that: 2 parties that ANy[don't have any] previous data of every different to collectively establish a shared secret key over an insecure communication. However, the protocol assumes the resister has finite computation power and depends upon procedure hardness of bound mathematical issues to realize secure key generation.

These bodies of cryptanalytic protocols reach procedure security. Recently, the notion of physical layer (PHY) based mostly key generation has been planned and also the ensuing approaches function various solutions to the key institution downside in wireless networks. supported the idea of reciprocity of antennas and magnetic attraction propagation, the channel responses between 2 transceivers is used as a supply of common randomness that's not offered to adversaries in different locations. Such supply of secrecy, that is provided b y the weakening method of wireless channels, will facilitate to realize information-theoretical security. This body of labor is copied back to the first information-theoretical formulation of secure communication [1] and knowledge theorists characterised the elemental bounds and showed the feasibleness of generating secrets mistreatment auxiliary random sources [2, 3]. However, they're the majority supported theoretical results and don't gift express constructions. To the most effective of our data, Hershey et al. planned the primary key generation theme supported differential section detection in [4]. Mistreatment multipath channels because the supply of common randomness, recent researches specialize in menstruation a preferred data point of wireless channel, i.e., received signal strength (RSS), for extracting shared secret bits between node pairs [5,6]. It's been incontestable that these RSS based mostly ways are possible on custom-made 802.11 platforms.

The state of the art, however, still suffers from major limitations. First, the key bit generation rate supported by these approaches is extremely low. This is often because of the very fact that the PHY based mostly key generation depends on channel variations or node quality to extract high entropy bits. Within the time intervals wherever channel changes slowly, solely a restricted range of key bits is extracted. The ensuing lo w key rate considerably limits their use given the intermittent property in mobile environments. To extend the key rate, Zeng et al. planned a key generation protocol by exploiting multi-antenna diversity [9]. However it additionally results in a rise within the quality of the transceivers. Second, the generated raw key bit stream has low randomness. This is often as a result of the distribution of the RSS measurements or estimates isn't uniform, which ends in unevenly possible bits once quantisation.
As cryptographic keys got to be as random as attainable so it's unfeasible to breed them or predict them, it's vital to confirm high entropy of the generated keys. However, the matter of a way to safely and expeditiously generate random key bits mistreatment channel randomness continues to be open. To beat the higher than limitations, this method focuses on a cooperative wireless system wherever there's AN attested and honest relay. Passive adversaries, i.e., eavesdroppers, are assumed during this system. The case once the snooper is collocated with the relay, that is shown to be the worst case snooper location supported the source-to-eavesdropper channel ratio (SNR), is studied. Lower and higher bounds on the key key rate between the 2 legitimate communicants with relevance the knowledge obtained by the snooper are derived for specific modulation and SNR conditions. In this, propose a gaggel authentication and key agreement protocol. The look of a key agreement protocol supported a completely unique and easy advantage distillation theme that exploits the physical channel randomness is studied. Style parameters are determined supported key rate bounds to optimize the potency of the protocol whereas making certain secrecy. Numerical examples and simulation studies are bestowed to demonstrate the performance of the cooperative key generation system.

The results show that the key rate is improved by one or two of orders of magnitude compared to the prevailing approaches. The fig.1 shows the system design of the planned work.

![Fig.1. Proposed Architecture Diagram](Image)

The rest of the paper is organized as follows: Section II discusses related work. Section IV provides the elaborated description of our planned cooperative key agreement schemes. Section V presents performance analysis and simulation results. Finally, Section VIII concludes the paper with future work.

2. RELATED WORK

To the most effective of our information, the primary key generation theme appropriate for wireless network was projected in [4]. In [4], the differential section between two frequency tones is encoded for key generation. Error management coding techniques square measure used for enhancing the irresponsibleness of key generation. Almost like [4], a method of using random section for extracting secret keys in associate degree OFDM system through channel estimation and division was recently projected in [8]. This paper characterized the likelihood of generating a similar bit vector between two nodes of signal-to-interference-and-noise (SINR) and division levels. A key generation theme supported extracting secret bits from correlate deep fades was projected in [5] and distinguished from the same work by exploitation received signal strength (RSS) because the random supply via a TDD link for the protocol style. Two cryptographic tools– data reconciliation and privacy amplification are wont to eliminate bit vector discrepancies as a result of RSS menstruation spatiality. The ultimate key agreement is achieved by leaky out borderline data for error correcting and sacrificing an exact quantity of entropy for generating nearly excellent random secret bits. In [9], the author’s projected two key generation schemes supported channel impulse response (CIR) estimation and RSS measurements. Totally different from [5], the 2 transceivers alternately send identified probe signals to every another and estimate the magnitude of channel response at consecutive time instants. The excursions within the fading channels are used for generating bits and therefore the temporal order of excursions is employed for key reconciliation. The ensuing sequence are additional filtered and amount employing a 1-bit quantizer, which ends up in low key bit rate. Impelled by observations from quantizing conjointly mathematician method, a lot of general key generation scheme was projected by exploiting empirical measurements to line division boundaries in [10].

Engaged on a similar RSS based mostly approach, [6] evaluated the effectiveness of RSS based mostly key extraction in real environments. It's been shown that as a result of lack of channel variations static environments don't seem to be appropriate for establishing secure keys, and node quality helps to come up with key bits with high entropy. The foremost recent work [11] projected an economical and clickable key generation theme that supports each pairwise and cluster key institutions. As a result of noise, interference and different factors within the key generation method, discrepancies could exist between the generated bit streams. Variants of this drawback are extensively explored below the names data reconciliation, privacy amplification and fuzzy extractors. In [12] projected the primary protocol to resolve the information-theoretic key agreement drawback between two parties that originally posses solely correlate weak secrets. The key agreement was shown to be theoretically possible once the data that the 2 bit strings contain regarding one another is quite the data that the snoop has regarding them. In [13] used error-correcting techniques to style a protocol that's computationally economical for various distance metrics. Supported the previous results, [14] projected a protocol that's economical for each parties and has each lower round complexity and lower entropy loss.

3. PROPOSED METHODOLOGY

3.1 System Model

In this module we tend to take into account secret key agreement protocol style for a three-node cooperative wireless communication system using a typical modulation theme. The most assumptions are as follows. The wireless communication system model is shown in Fig. 1. The system contains 2 legitimate parties Alice and Bob, yet as a relay R for cooperation. The relay within the system is concerned within the key agreement method to realize a better key rate via cooperation. Each the
Proposed Group Authentication Protocol and Noise reduction Quasi-static fading for all inter-node channels is assumed, and therefore the noise at completely different locations is freelance and identically distributed (i.i.d.) Additive White Gaussian Noise (AWGN). So in every transmission block (frame) containing N symbols, the received SNR of all the inter-node channels is constant. Denote the received SNRs for the AR, rb and AB channels by random variables \( \Gamma_1, \Gamma_2 \) and \( \Gamma_D \), severally. The fading statistics follow a selected distribution, e.g. Nakagami-m fading. In a very explicit time interval we've got random realizations \( \gamma_1, \gamma_2 \) and \( \gamma_D \) for \( \Gamma_1, \Gamma_2 \) and \( \Gamma_D \) severally. During this module, we tend to offer the main points of the cluster authentication and key agreement protocol. So as to realize this aim, there are 3 phases within the planned protocol: cluster initialization, authentication information distribution, and mutual authentication and key agreement.

Group Initialization

In the group initialization phase, every device includes a permanent ID (PID), like international mobile subscriber number (IMSI). His PID may be a long personal identity that identifies device and will be put in within the device by the provider so as to permit the MTC device to register in a very 3GPP network. At an equivalent time, we tend to assume that every device has pre-shared a secret key with 3GPP CN, and these MTC devices kind many teams supported bound principles, then the provider provides a group key (GK) to every group for authentication. We tend to produce an index table to manage data of devices and group; the index table contains fields of group identity, device identity (PID) for every device, and initial values.

Authentication Data Distribution

Client C is that the party initiating the exchange. Within the wireless context, C is sometimes a MS requesting to be affiliated with the shopper C. within the wireless context, S grants C access to resource (network visited whereas roaming). As noted, C’s credentials (i.e. key k) don’t seem to be issued by S, and are unknown to him. Instead, S receives (possibly batched) one-time authentication vectors av from Key Server. ECDH may be a key agreement protocol that enables two parties to ascertain a shared secret key which will be used for personal key algorithms. Each parties exchange some public data to every alternative. Exploitation this public information and their own personal information, these parties calculates the shared secret. Any third party, who doesn't have access to the personal details of every device, won't be ready to calculate the shared secret from the obtainable public data.

EAP- AKA Protocol

EAP-AKA provides mutual authentication between the user instrumentation (UE) and authentication, authorization and accounting (AAA) server. From step one to four the affiliation is established with EAP request/identity and therefore the subscriber is known to the house subscriber server (HSS). From step five to six, the AAA server requests once more the user identity as immediate nodes will modify user identity (IMSI) enclosed in EAP response/identity message. Therefore, if the UE receives EAP request/AKA identity message, the UE ought to send EAP response/AKA identity message that should contain an equivalent user identity enclosed response/identity message to the AAA server. The AAA server can use user identity received from EAP response/AKA identity message within the remainder of the authentication and key agreement procedure. In Step 7, the AAA server checks the WiFi access profile and verifies that the subscriber is permitted to use the WiFi service. From step seven to fifteen the challenge/response mechanism is applied to perform the mutual authentication between the AAA server and therefore the UE. As the results of the success of the mutual authentication the master session key (MSK) is shipped to the AP successfully message.

Proposed EG-AKA Protocol

In our planned protocol, we tend to assume the following: A secure channel is established between the AAA server and therefore the HSS. The UE will establish the ID of AAA server and AP within which the UE in its vary of coverage. 5.2 Procedure:

Step 1. UE searches for the ID of the meant AP, once it finds the AP, the UE sends begin message to start out the authentication mechanism.

Step 2. The AP requests the UE Identity.

Step 3. The UE do Generate (RAND) \( \rightarrow \) a random worth

Generate (KTEMP) \( \rightarrow \) a short lived key

KTEMP=EKUE-HSS (TU).

Encrypts its ID (IMSI), concatenated with the timestamp TU. IDenc=EKTEMP (IMSI||TU).

UE sends its encrypted ID (IDenc), timestamp (TU), ID of the access point (IDAP) and therefore the ID of the home server (IDHSS) to the HSS.

Step 4. The HSS do

Retrieves a visible header within the IDenc referred to as (key-indicator) and finds the corresponding key to the indicator (KUE-HSS).

Calculates KTEMP=E KUE-HSS (TU).
Decrypts $\text{IDenc}$, retrieves timestamp ($\text{TU}$) and compare it to the ($\text{TU}$) received in step (5) and checks that ($\text{TU}$) is that the same.

Generates ($\text{NHSS}$)→ a random number

Computes $\text{AUTH-AAA}$ as follows: $\text{AUTH-HSS}=\text{MACKUE-HSS} (\text{NH-SS}||\text{ID-HSS}||\text{ID-AP}||\text{ID-AAA})$

Step 5. HSS Sends ($\text{NHss}$, $\text{KTEMP}$ , $\text{IDAP}$, $\text{AUTH-HSS}$) to the WLAN-AAA .

Step 6. The WLAN-AAA do
Stores $\text{KTEMP}$ and $\text{IDAP}$.
Generates ($\text{NAAA}$)→ a random worth
Computes: $\text{AUTH-AAA}=\text{MACKTEMP} (\text{NAAA}||\text{NHSS}||\text{ID-HSS}||\text{ID-AP}||\text{ID-AAA})$.
Generates a random worth $a$ and computes $aP$ on $E$.

Step 7. The WLAN-AAA Sends the ($\text{NHSS},\text{NAAA},\text{AUTH-AAA},\text{AUTH-HSS},\text{ap}$) to the UE.

Step 8. The UE do
attest HSS by verificatory $\text{AUTHHSS}$.
attest WLAN-AAA by verificatory $\text{AUTH-AAA}$.
Generates a random range ($\text{NUE}$).
Generates a random worth $b$ and computes $bP$ on $E$.
Computes $\text{KUE-AAA}=\text{fKTEMP} (abP)$.
Computes $\text{AUTHUE }=\text{MACKUE-AAA} (\text{NUE}||\text{NAAA}||\text{NHSS}||\text{ID-HSS}||\text{ID-AP}||\text{ID-AAA})$.
Computes $\text{CK}$, $\text{IK}$, and $\text{MSK}$.

Step 9. UE Sends ($\text{AUTHUE}$ , $bP$ , $\text{NUE}$) to WLAN-AAA server.

Step 10. The WLAN-AAA do
Computes $\text{KUE-AAA}=\text{fKTEMP} (abP)$.
Authenticates UE by verificatory $\text{AUTHUE}$.
Computes $\text{CK}$, $\text{IK}$ and eventually $\text{MSK}$.

Step 11. The WLAN-AAA sends the $\text{MSK}$ concatenated with $\text{IDAP}$ with $\text{EAP}$ success message to the $\text{AP}$, and additionally sends the $\text{MSK}$ concatenated with $\text{IDAP}$ encrypted with $\text{KUE-AAA}$ to the UE, that the $\text{MSK}$ won't be compromised within the air interface between the $\text{AP}$ and therefore the $\text{UE}$.

Step 12. The $\text{AP}$ stores the $\text{MSK}$ and forwards ($\text{MSK}||\text{IDAP}$) with the $\text{EAP}$ success message to the $\text{UE}$.

Step 13. The UE decrypts the $\text{MSK}$ received from the $\text{AP}$ and verifies if it's equals the $\text{MSK}$ calculated in step (7) and additionally verifies that the $\text{IDAP}$ received equals the $\text{IDAP}$ sent in step (3). If the verification is correct, then the procedure of the authentication and key agreement is successful and therefore the UE will use WiFi services firmly via the $\text{MSK}$.

Formal Verification
The primary goal of our planned protocol is to produce mutual authentication and key agreement services between devices. We tend to test our protocol exploitation formal security verification module. We are able to verify that the planned protocol can offer a self-made mutual authentication between devices. Since these random numbers employed in every authentication procedure are completely different, even though an assaulter acquires a random range in an authentication procedure, he still cannot pretend challenge messages by reusing the random range in a very new authentication procedure.

4. RESULTS AND DISCUSSIONS

In this section, the proposed EG-AKA result is evaluated and their performances are discussed and it is compared with existing system of EAP-AKA.

4.1 Network Lifetime
The lifetime of the network is defined as the time at which the first node failure occurs, that is, the time at which some node’s energy reserve is reduced to zero. The main point here is to determine the lifetime for numerous routing schemes. It can be seen that in the Fig.3, the lifetime of the network depict a reducing returns anytime the size of the network start to grow bigger. When this trend is compared with some schemes, an increment of network lifetime with EG-AKA is significantly higher than EAP-AKA.

4.2 Average Energy Consumption
It measures the average difference between the initial level of energy and the final level of energy that is left in each node. Energy consumption of the node is the subsequent metric to be conducted. From the Fig.4 illustrated, EG-AKA energy consumption is much lesser when compared to other EAP-AKA routing scheme. It keeps node energy consumption of node at reduced state through increment of network size normally occurs. The energy efficiency of EG-AKA is more consistent as the results shows from the experiment conducted and the effect of increasing the size of the network shows smaller effects and comparing it to other routing schemes their performances diminishes when the network size becomes bigger.
4.3 Average Control Packet Overhead

It is the ratio of the average amount of control message treated by the node and the amount of data packets received by the sinks. There are several routing schemes each having distinct technique and if a network is much bigger, it is necessary to needs greater amounts of exchange of control illustrate messages so as to be able to find and create more routes. This implies greater amount of energy is consumed and needed during the initial construction phase. Further when the network is a bigger one, it means it will take extensive time distance that separates the sink and the source nodes. There are many intermediate nodes which have to be navigated to enable a data packet to arrive at the destinations sink nodes. Control message overhead of several routing are illustrated in the Fig.5 and to get this value is through computation of two elements, that is, the ratio of the average amount of control message treated by the node and the amount of data packets received by the sinks. Here the control message overhead portrays directed diffusion as having to expend greater amount of energy during transmission and receiving control messages when compared with another routing schemes, because it needs periodic interest broadcast and path reinforcement which consumes extra energy.

![Fig.5. Average Control Packet Overhead](image)

4.4 End-to-end Delay

It defines as the average time taken by a data packet to arrive at the destination. Only the data packets that successfully delivered to destinations that counted. The average packet delay is described in the Fig.6, showing that in comparison with another schemes the EG-AKA having the shortest delay is a great benefit to the scheme. Through the use of EG-AKA, as estimated the data packet is routed through several node-disjoint paths, so with this method the network congestion and the transmission interferences possibilities are mostly avoided.

![Fig.6. End-to-end Delay](image)

4.5 Packet Delivery Ratio (PDR)

Packet Delivery Ratio is the ratio of the number of delivered data packets to the destination and the number of the send packets by the source as shown in Equation below. This illustrates the level of delivered data to the destination.

\[
PDR = \frac{\sum \text{Number of packet receive}}{\sum \text{Number of packet sent}}
\]

The packet delivery ratio is described in the Fig.7, it is simply the ratio of the number of delivered and transmitted data packet to the destination. It is usually portrays the state of data packets sent to the destination. Through the use of dispersion method reliability is attained, implying EG-AKA performs much better by attaining the best delivery ratio in comparison with existing EAP-AKA scheme.

![Fig.7. Packet Delivery Ratio](image)

4.6 Throughput Evaluation

Throughput is defined as the total number of packets delivered over the total simulation time. Mathematically, it can be defined as:

\[
\text{Throughput} = \frac{N}{1000}
\]

Where \(N\) is the number of bits received successfully by all destinations.
Fig. 8 shows the throughput comparison of the proposed EG-AKA protocol approach and the existing EAP-AKA. It is noted that the proposed EG-AKA protocol attains higher throughput when compared with the existing EAP-AKA. The reason is that, the probability to meet the desired event data in a short hop count is very high in such a way.

5. CONCLUSION

In this paper, we tend to propose a bunch authentication and key agreement protocol beneath the EAP framework, named EG-AKA. To the most effective of our data, there's no protocol within the current literature that handles specific group access authentication. The planned EG-AKA protocol not solely enhances security on the premise of Mun's protocol, however additionally styles specific cluster authentication mechanism for wireless networking. Formal verification and security analysis show that the planned protocol is secure and fulfill its style goals. Elaborate evaluations of performance illustrate that the planned protocol achieves higher performance in terms of transmission and sign overhead compared with many existing protocols. As a future work, we are going to take into account additional sensible group authentication protocol supported symmetric cryptography for resource-constrained devices in heterogeneous networks.

REFERENCES