Fast Initial Link Setup In IEE802.11AI Using Son Algorithm

Mr.S.Kannan [1], G.Chithra [2]
[1] Assistant Professor, Dept of CSE
[2]Dept of CSE
[1, 2] Sembodai Rukmani Varatharajan Engg College, Sembodai, Nagapatnam-614809

Abstract- *The increasing deployment of smart devices has proved that Internet of Things (IoT) is an overwhelming trend for the next era. IEEE 802.11ai, a specification belonging to 802.11 Wireless Local Area Network protocol family, has been recently released to support the long-range, low-power and low-rate wireless communication among smart devices used in IoT systems. However, security requirements on the energy constrained devices have plenty of features different from the traditional devices. The overhead of messages has to be minimized, even though the entire performance might be compromised. There is an upcoming solution towards this problem discussed in IEEE group, which was described in IEEE 802.11ai, where the Fast Initial Link Setup has been defined as a novel methodology aiming at establishing fast, stable and secure links among smart devices. Wireless communication is to address the security issues of the IEEE 802.11ai specified wireless networks with a proposal of an enhancement to the authentication process in the setup procedures for the IEEE 802.11ai specified low power driven wireless sensor networks. The security functionality of the proposed solution is derived by BAN logic while the performance of the solution is evaluated by simulation experiments to demonstrate the advantages of the proposed solution.*

Keywords- Fast Initial Link Setup;BAN logic;802.11ai

I. INTRODUCTION

New generation of communication technologies, the control data and network performance measurements in the Operation and Maintenance (O&M) subsystem grow in both volume and speed. A larger number of users and quantity of transferred data means a larger amount of measurements. In addition, the higher demand for quality and larger bandwidths pushes for a faster rate of generation and consumption of these data. Downtimes due to problems that are not solved quickly or incorrect optimization cause a high opportunity cost and increased overall O&M costs.

For these reasons, the Next Generation Mobile Network (NGMN) Alliance and the Third Generation Partnership Project (3GPP) defined Self-Organizing Networking(SON) as a set of principles and concepts to add automation to mobile networks so that they require less maintenance than traditional networks while improving Quality of Service (QoS). SON functions take as input the measurements generated by mobile networks, and produce output that depends on the purpose of the function.

Wireless networks have increasingly grown in complexity with the introduction of new technologies and services. The scenario in the years to come will be characterized by its heterogeneity, as different Radio Access Technologies (RATs) (GSM, UMTS, and LTE), transmission solutions, and network architectures (macro-, micro-, pico-, and femto-cells) will coexist. In this context, operators must face the challenge of offering new high quality services, while reducing both Capital Expenditure (CAPEX) and Operational Expenditure (OPEX). However, as the number of technologies, services, cell types, and operators grows, network planning and operation become more complex. The solution to cope with this complexity is to automate most network procedures, with the final aim of having a network that is autonomously managed. However, nowadays the number of procedures, e.g. related to optimization and fault management, that are manually carried out is still considerable. In this context, Self-Organizing Networks (SONs) are those networks capable of self-configuring, self-optimizing, and self-healing. The deployment of LTE worldwide and its operation in parallel with GSM/UMTS/HSPA are pushing operators to develop SON mechanisms if they want to remain competitive. Furthermore, the large scale deployment of small-cells and their interaction with macro cells make SON functions essential for operating such complex networks.

SON reduces OPEX by means of automating tasks that are currently manually performed by highly experienced staff. In addition, SON also contributes to CAPEX reduction, thanks to a more efficient use of network elements and resources. Consequently, better coverage, capacity, and quality can be achieved with lower investment.Functionalities that automate the solution of problems, reducing human

intervention and minimizing downtime.Self-healing includes fault detection, diagnosis, compensation, and recovery it includes functions to cope with service degradation or outage, including fault detection and diagnosis and mechanisms for outage compensation.

Currently, there is a large fragmentation in references related to self-healing. First, technical documents, including scientific papers, project deliverables, standards, whitepapers, etc., use different terminology. Even the simplest concepts are used with different meanings. For example, in some references the term "fault" only refers to hardware problems; in some technical documents "fault" also includes all faults related to network elements, not only related to hardware, but also to software; in other references, a fault can happen not only in a network element, but it can also be caused by wrong global configuration or external factors, e.g. interference or coverage problems. Another example of confusion is the difference between self-healing and self-optimization. Although in principle the difference seems obvious, the boundary is not so clear in some cases.

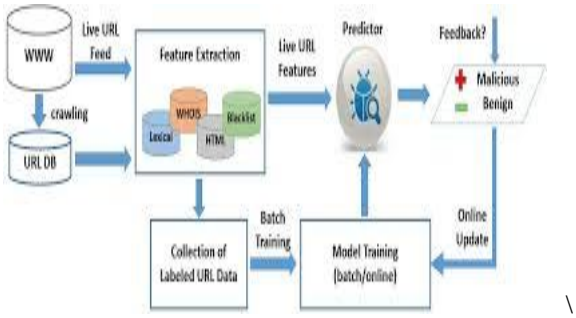
For example, when there are problems in a cell due to a bad parameter setting, is parameter tuning a function belonging to self-healing or to self-optimization? The answer to this question is different depending on the technical document. Second, references normally focus on a given function within those composing self-healing, e.g. cell outage compensation, in a specific scenario and use case. Although, in most cases, the existence of other functions is acknowledged, self-healing as a whole is not presented in most documents, but only a function is studied in isolation.The consequence is that the proposed solution may not be valid or optimal when integrated with the rest of self-healing functions. Therefore, there is a need for systematizing studies on self-healing and for unifying the fragmentation on existing references. The purpose of this article is to propose a conceptual framework for self-healing, where the main terms and functions, which are ambiguously used in literature, are clarified and unified. In addition, the state of the art will be presented and the main challenges in the topic will be discussed.

Self-healing aims to automate troubleshooting, which is one of the most important O&M tasks.The main objective of troubleshooting is finding and fixing malfunctions in the network. In the currently deployed LTE networks, this task is manually done by monitoring some variables that reflect the state of the network. Self-healing functions include data processing algorithms that analyze O&M data in order to identify and fix problems. Some attempts at defining an implementation for self-healing functions have been made using Knowledge-Based Systems (KBSs), such as Bayesian networks, fuzzy logic controllers, or case-based reasoning for automatic diagnosis. These systems have been proposed theoretically without acknowledging the problems inherent to large databases. When data largely increase, traditional processing techniques have very poor performance. The big data paradigm deals with this type of dataset by applying new techniques that exploit the latest hardware and software innovations.

In mobile networks, performance measurement data have already passed that threshold; therefore, it must be studied through the paradigm of big data. a general vision of big data for SON functions was given, without going into details on each SON functionality. This article goes one step further, focusing on self-healing functions. In particular, in this article, self-healing is reframed as a big data problem, and some specific requirements for the development of big-data-compliant self-healing functions are proposed.to further illustrate these principles, some use cases are shown, where modifications on previously existing algorithms that work with big data compliant inputs are proposed in order to use big data processing techniques.

II. OVERVIEW OF APPROACH

Given an unknown program to analyze, We wish to automatically determine whether it exhibits in a secured process and its behaviour.In this work is having following process like to create FKR key for authenticating secure members. A novel integrated detection and diagnosis framework is presented that can identify anomalies and find the most probable root cause of not only severe problems but even smaller degradations as well.[1].To perform our automatic authentication process we run a series of automated tests which is performed by the test engine. For each test, we generate events that introduce sensitive information in to the guest system. MapReduce is a programming model and an associated implementation for processing and generating large data sets. Simplified Data Processing on Large Clusters[7]. Continuous versus Discrete Model in Auto-diagnosis Systems for Wireless Networks. (Radio Access Network)The proposed system is based on the analysis of Key Performance Indicators (KPIs) in order to isolate the cause of the network malfunction[13] a highly scalable data streaming infrastructure for CEP, which to parallelize the load carries on breaking the query into sub-queries and assigns each one of the sub-queries a computing



Sub-cluster. The author proposes and investigates different strategies for the formation of clusters[5]. In order to improve the performance of authentication, as our major contribution, we propose a new mechanism called Fast Key Reestablishment (FKR) to simplify the authentication and key generation process while keeping the same security level of the FILS. It provides a faster way to accomplish authentication and session keys generation after first round of communication. The security functionality of the authentication and key generation process's derived by BAN logic and the performance is evaluated by the simulation experiments.

A distributed Privacy-Preserving Access Control scheme for sensor networks, which is the first work of its kind [10]. Users in DP2AC purchase tokens from the network owner whereby to query data from sensor nodes which will reply only after validating the tokens. The use of blind signatures in token generation ensures that tokens are publicly verifiable yet un linkable to user identities, so privacy-preserving access control is achieved [10].

A central component in DP2AC is to prevent malicious users from reusing tokens, for which we propose a suite of Distributed Token Reuse Detection (DTRD) schemes without involving the base station. These schemes share the essential idea that a sensor node checks with some other nodes (called witnesses) whether a token has been used, but they differ in how the witnesses are chosen.

III. DESIGN AND IMPLEMENTATION

System design concentrates on moving from problem domain to solution domain. This important phase is composed of several steps. It provides the understanding and procedural details necessary for implementing the system recommended in the feasibility study. Emphasis is on translating the performance requirements into design specification.

The design of any software involves mapping of the software requirements into Functional modules. Developing a real time application or any system utilities involves two processes. The first process is to design the system to implement it. The second is to construct the executable code. Software design has evolved from an intuitive art dependent on experience to a science, which provides systematic techniques for the software definition. Software design is a first step in the development phase of the software life cycle. Before design the system user requirements have been identified, information has been gathered to verify the problem and evaluate the existing system. A feasibility study has been conducted to review alternative solution and provide cost and benefit justification. To overcome this proposed system is recommended. At this point the design phase begins.

The process of design involves conceiving and planning out in the mind and making a drawing. In software design, there are three distinct activities: External design, Architectural design and detailed design. Architectural design and detailed design are collectively referred to as internal design. External design of software involves conceiving and planning out and specifying the externally observable characteristics of a software product.

FILS Authentication

After the first round of the FILS authentication has been executed, the PMK is settled and can be used for a certain period of time, while the PTK could be changed and renegotiated for the rest of the session. The FKR scheme provides a 2-way method to reestablish a new PTK set with the same PMK serving as an input keying material. During the 2-way handshake, the STA and the AP can renegotiate a new PTK session and confirm each other again without exposing the 4-way handshake. Thus, it is assumed that the STA and the AP have already shared a PMK and PTK from the previous authentication. By the FKR, they have agreed on a same hash function.

Frame Decryption

Upon receipt, the AP uses PTK derived in previous session to decrypt the frame from the STA and acquire Ns. The AP then uses the same way to calculate PTK′. Once PTK′ is calculated, the AP is able to verify the Ns encrypted with PTA′ in the first message. If it is verified to be successful, the AP can construct the second message with the GTK and the current Key RSC as well as AP nonce NA. Through a successful verification, the STA has the knowledge of the PMK, the previous used PTK, and the freshly generated nonce for this PTK′, the AP can trust the newly calculated PTK′ as the new PTK for the next session. The second message sent by the AP proves that the AP accepts the new PTK′ and has the knowledge of PMK and previous used PTK.

Verification

To verify the security functionality of the proposed FKR scheme, we first prove the logic correctness of the FKR by using BAN logic.

Security analysis

The proposed FKR serves as the FILS's substitute to achieve the FILS functions. Firstly, it confirms the PMK on each side. Secondly, the STA and the AP can mutually authenticate each other. Thirdly, both sides derive a fresh session key PTK. Finally, it distributes the GTK to the STA. The FKR requires the AP to calculate the new PTK with the PMK and the new nonce received. It proves that the AP has the knowledge of the PMK. From the information encrypted with new PTK in the first message, it is apparent that the STA has the knowledge of the PMK. And the knowledge of the old PTK as well as the knowledge of the PMK makes them authenticate each other. After 2 messages exchanged, both sides demonstrate that both of them accept the newly calculated PTK. The second message contains the GTK distributed to STA.