

<http://ansinet.com/itj>

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Enhanced Intrusion Detection System for PKMv2 EAP-AKA used in WiBro

¹Sang-Guun Yoo, ²Soojin Lee, ²Yunho Lee, ¹Yeong-Kyu Yang and ¹Juho Kim

¹Department of Computer Science and Engineering, Sogang University, Seoul, Korea

²Department of Defense Information Science, Korea National Defense University, Seoul, Korea

Abstract: WiBro (Wireless Broadband), the service based on the IEEE 802.16e (mobile WiMAX) standard, is an emerging wireless broadband Internet technology providing full mobility through open IP based network with various types of terminals. The security of WiBro is based on the IEEE 802.16e-2005 with new version of PKMv2 (Privacy Key Management version 2) which allows the use of EAP-AKA protocol for authentication. However, the enhanced security solution does not make WiBro free from attacks creating the need for additional security measures. Present study proposes an option of such security measure in form of an intrusion detection system for the authentication phase of WiBro. The proposed system makes use of formalized specifications of the normal operation of the PKMv2 EAP-AKA authentication to detect misbehavior messages being transmitted over the network. Once defined the architecture and design, the proposed intrusion detection system was developed and implemented in an experimental network to verify its capabilities by simulations. Simulations show how the proposed solution detects existing attacks and provides capabilities to detect new attacks that violate the normal flow of EAP-AKA protocol. The specification-based characteristic of the proposed intrusion detection system allows effective detection of unknown attacks which is very useful in a complicated WiBro environment with the potential to be a victim of new type of attacks in the future.

Key words: Wibro, intrusion detection, authentication, network security, denial of service, EAP-AKA

INTRODUCTION

Since mobile Internet services are becoming more and more popular, different kinds of new technologies have emerged. A typical example of such technology is WiBro (Wireless Broadband) which improves the limitations of the existing mobile Internet (Lee *et al.*, 2006; TTA, 2007). WiBro, a South Korean technology, is one of the newest varieties of mobile wireless broadband access based on the IEEE 802.16e standard as mobile WiMax (Shahid *et al.*, 2008). The IEEE 802.16e and Mobile WiMax have become popular because they provides benefits such as wide radio range and high speed allowing the provision of different kind of services (Wu, 2010; Bahaman *et al.*, 2011; Ei and Furong, 2010; Eshanta *et al.*, 2009). WiBro also uses the IEEE 802.16e standard but it offers enhanced characteristics such as superior mobile connectivity allowing mobile devices to communicate at speeds of up to 37 miles per h (TTA, 2007). Because of its features, WiBro is considered to have the potential to compete in the 4G (4th Generation) wireless communication market. Security of WiBro is based on the IEEE 802.16e-2005 standard (IEEE, 2005) which includes an enhanced version of PKM: Privacy Key Management version 2 (PMKv2).

Authorization key is now generated using values delivered by both parties using well known standards

such as RSA and EAP (Extensible Authentication Protocol) where it initially was done only by the base station. Additionally, base station is extended with a certificate, allowing for mutual authentication with the mobile station which was missing in PKMv1. Finally, random nonces are incorporated in order to avoid replay attacks.

IEEE 802.16e and TTAS.KO-06.0082 (TTA, 2005) standards recommend RSA based on X.509 certificates and EAP as authentication methods for WiBro and describe the mobile station as the main body of authentication procedure. However, mobile station does not safely manage user's private information and important key value without physical security equipment or security platform for itself. For this reason, TTA (2006) suggests the mutual authentication mechanism based on PISIM (Portable Internet Subscriber Identity Module) using EAP-AKA (Authentication and Key Agreement).

However, even though WiBro uses enhanced security schemes supported by PKMv2, it does not guarantee the reliability of whole authentication process. Being more specific, the authentication phase of PKMv2 EAP-AKA suffers from vulnerabilities that an attacker could take advantage; these vulnerabilities are analyzed in the subsection called Vulnerabilities of WiBro, later. But the provision of an agile solution to those vulnerabilities becomes difficult because they are already

part of the WiBro standard. Therefore, an intrusion detection system becomes a suitable safeguard to alleviate this problem.

Intrusion detection techniques can be broadly classified into the categories of misuse detection, anomaly detection and specification based detection (Sekar *et al.*, 2002). Misuse detection (Porras and Kemmerer, 1992; Kumar and Spafford, 1994) which detects known misuses accurately, is not very effective against unknown attacks. Anomaly detection (Anderson *et al.*, 1995; Forrest *et al.*, 1997; Ghosh *et al.*, 1999; Raja *et al.*, 2008) handles unknown attacks better but can generate a lot of false positives and hence is not deployed widely. The specification-based approach (Tseng *et al.*, 2003; Lee and Lee, 2010) is similar to anomaly detection in the sense that it detects activities executed outside the boundaries of a normal pattern; however, it provides advantages such as the detection of novel attacks and maintenance of a low degree of false alarms.

Present study proposes an enhanced specification-based intrusion detection system for PKMv2 EAP-AKA authentication used in WiBro. Enhancement of the previous solution (Lee and Lee, 2010) proposed by some of authors of this paper is proposed including two major aspects: (1) addition of the fast re-authentication and error cases of EAP-AKA defined in (Arkko and Haverinen, 2006) and (2) development of an upgraded intrusion detection system with user friendly visual interface and multiple sessions monitoring capabilities.

SECURITY IN WiBro

Security of WiBro is mainly based on the IEEE 802.16e security specification which is mainly located

within the MAC layer called the security sub-layer (IEEE, 2005). The goal of the security sub-layer is to provide access control and confidentiality of the data link (Fig. 1) by providing authentication, secure key exchange and encryption.

The previously mentioned IEEE standard allows the use of RSA based on X.509 certificates and EAP as service authentication methods. However, the EAP-AKA protocol using PSIM (Portable Internet Subscriber Identity Module) is the most widely used in WiBro implementation (TTA, 2006).

Vulnerabilities in WiBro: Even though the presence of the security features in IEEE 802.16e, WiBro suffers from several security flaws which are detailed in researches such as (Lee and Lee, 2010; Sakib *et al.*, 2010; Bhargava *et al.*, 2009; Altaf *et al.*, 2008; Malekzadeh *et al.*, 2009). This subsection describes some of those vulnerabilities that affect the PKMv2 EAP-AKA authentication process used in WiBro.

- Denial of Service attack based on EAP-Failure message: in this attack, the attacker camouflages itself as an authentic base station and sends PKMv2 EAP-Transfer (EAP-Failure) message to obstruct connection from mobile stations. The mobile station when receives the PKMv2 EAP-Transfer (EAP-Failure) messages concludes that the authentication has failed and terminates its connection
- EAP-Failure inducing Denial of Service attack: in this attack, the attacker uses a spoofed mobile station to send messages to the base station to induce generation of PKMv2 EAP-Transfer (EAP-Failure) having as a goal the blocking of access to services of

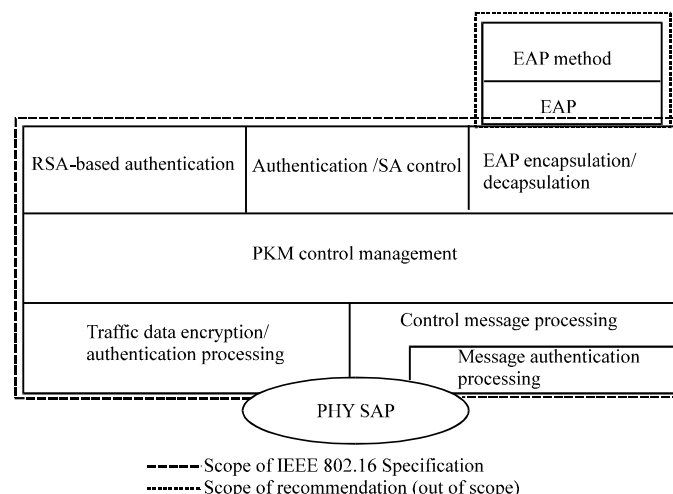


Fig. 1: IEEE 802.16 security sublayer

authentic devices. Messages which may induce PKMv2 EAP-Transfer (EAP-Failure) message are as follows:

- PKMv2 EAP-Transfer (EAP-Response/AKA-Authentication-Reject)
- PKMv2 EAP-Transfer (EAP-Response/AKA-Notification)
- PKMv2 EAP-Transfer (EAP-Response/AKA-Client-Error)
- Denial of Service attack based on PKMv2 EAP-Start messages: the mobile station must send a PKMv2 EAP-Start message to the base station to request authentication in a EAP based authentication process. The base station which receives the message identifies the beginning of the authentication and requests the identity to the mobile station. Once, initiated the authentication process, the base station ignores other PKMv2 messages coming from the same mobile station. This vulnerability is exploited in this attack. The attacker after camouflaging itself as an authentic mobile station sends periodically requests for EAP authentication. The PKMv2 message sent by the authentic mobile station will be ignored by the base station provoking the isolation of the mobile station
- RES-CMD Replay Attack: the RES-CMD message contains the Reset Command which suspends all communication of the mobile station and forces connection re-initialization. RES-CMD messages do not include serial number, time information or arbitrary unique information. Therefore, the attacker can capture a RES-CMD message transmitted to a mobile station and can replay to the mobile station again to induce the reset of communication
- RES-CMD induction attack based on replay: additional to the previous attack, the attacker can induce the base station to send RES-CMD messages. The attacker can capture a message sent by an authentic mobile station and replay it continuously to the base station. The base station, after detecting the misbehavior, concludes that the mobile station is in malfunction and sends a RES-CMD message to the mobile station. The mobile station receives the message and resets the communication. The possibility of success of this attack depends a lot on how manufacturer have implemented the WiBro devices. This is because the standard asks for the transmission of a RES-CMD message when the mobile station does not respond or have constant problems; however, it does not specify details of constant problems

- Flooding attack in EAP-AKA authentication process: when the EAP-AKA authentication method is applied, the authentication server forwards the request for authentication of users to the authentication center (AuC) to obtain the authentication vector. The authentication servers and mobile stations use a challenge response communication for mutual authentication. The attacker can send arbitrary payload with a valid EAP header format randomly. The base station will recognize as valid messages and will forward them to the authentication server. In this attack, the attacker sends big amount of messages to make unstable the availability of the authentication server and AuC
- Resynchronization looping Denial of Service attack: the attacker uses a spoofed mobile station to periodically send PKMv2 EAP-Transfer (EAP-Response/AKA-Synchronization-Failure) messages to the base station to force the base station to cause the transmission of PKMv2 EAP-Transfer (EAP-Request/AKA-Challenge) messages. This attack provokes the base station to block access to normal services from the authentic mobile station

ENHANCED INTRUSION DETECTION SYSTEM FOR WiBro

Specification-based monitoring evaluates the behavior of objects with their connected security specifications that capture the correct behavior of the objects. The specifications are usually constructed based on the security policy, functionalities of the objects and object's expected usage. As the specifications are concerned with the correct behavior of objects, specification-based detection does not limit itself to detecting just known attacks but also any attack that changes the normal behavior of objects. The specification-based detection approach has been successfully applied to monitor security critical programs and protocols in researches such as Tseng *et al.* (2003), Gill *et al.* (2006), Tseng *et al.* (2006), Ko *et al.* (2001) and Jha *et al.* (2010).

The proposed solution uses the previously mentioned specification-based approach to detect the misbehaving messages. The specification of the normal message flows of PKMv2 EAP-AKA is defined and then intrusions by filtering messages that does not correspond to such specification are identified.

System architecture: Figure 2 shows the architecture of the proposed intrusion detection system. It works as a network based intrusion detection system attached to the base station infrastructure. It is composed of network

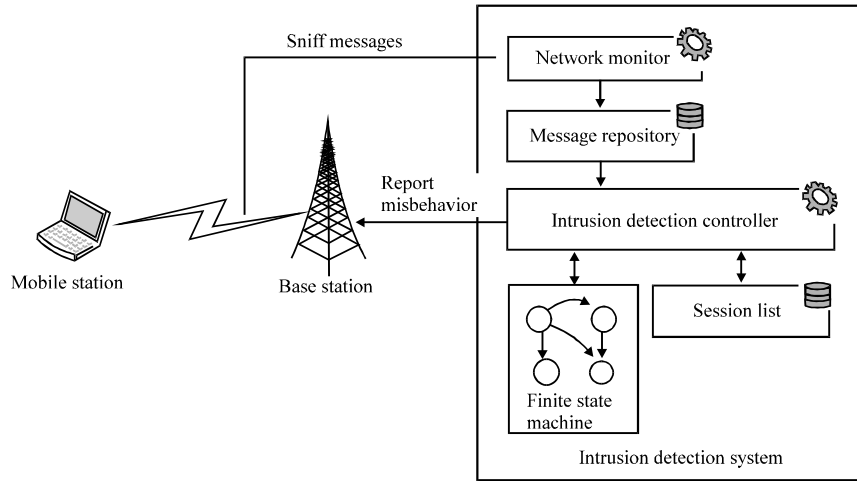


Fig. 2: Architecture of the proposed intrusion detection system

monitor, message repository, intrusion detection controller, session list and finite state machine.

Network monitor: The network monitor is responsible to sniff the network and capture new PKMv2 EAP-AKA messages. Pseudocode 1 below illustrates its main functionalities. The network monitor works in promiscuous mode to listen to all messages and verifies if the message is a PKMv2 EAP-AKA message; if so, the message is stored in the message repository.

Pseudocode 1: Network Monitor

```

while (system is up) {
    Wait (until hears message M being sent into channel);
    if (M's type is PKMv2 EAP-AKA message) {
        Store M in HISTORICAL_MESSAGE_REPOSITORY;
        Store M in ACTIVE_MESSAGE_REPOSITORY;
    }
    else
        Delete M
}

```

Message repository: This is a database containing the captured PKMv2 EAP-AKA messages. It is divided into two sections: (1) historical message repository which contains all captured messages used for log functionalities and (2) active message repository which contains the non-processed messages by the intrusion detection controller.

Intrusion detection controller: This component is the administrator of the system. Pseudocode 2 below describes the main process executed by the intrusion detection controller. It takes each non-processed PKMv2 EAP-AKA message from the active message repository and gets its Connection Identifier (CID). In WiBro, communications between a mobile station and the base

station are performed using CIDs; CIDs are generated for each connection after a series of ranging and registration steps in the initialization process. Once gotten the CID, its existence is verified in the active session list; if such CID is not found then a new register is inserted in the session list. The intrusion detection controller then verifies the validity of the message by using the finite state machine of the session. Details of how the finite state machine is used are explained in section finite state machine. If the message is not valid an alarm message is sent to the base station to inform about the intrusion. Once processed the message, the message is deleted from the active message repository.

Pseudocode 2: Intrusion Detection Controller

```

while (system is up) {
    var session CID, found;
    For each message M in ACTIVE_MESSAGE_REPOSITORY {
        sessionCID := get CID of M;
        if not(sessionCID is in ACTIVE_SESSION_LIST) {
            Create a register in HISTORICAL_SESSION_LIST with
                sessionCID;
            Create a register in ACTIVE_SESSION_LIST with
                sessionCID;
            Generate a instance of FSM for the new session;
        }
        Verify M using the session's FSM;
        if (M is not valid) {
            Log intrusion;
            Send an intrusion alarm to the base station;
            Delete register from ACTIVE_SESSION_LIST;
        }
        Delete M from ACTIVE_MESSAGE_REPOSITORY;
    }
}

```

Session list: This is a database containing the list of PKMv2 EAP-AKA sessions between mobile stations and the base station. As well as the message repository, it is divided into two sections: (1) historical session list which

contains the history of all sessions for log purpose and (2) active session list which contains the active sessions currently in process.

Finite State Machine (FSM): This is the core of the intrusion detection algorithm. An instance of the FSM is created for each communication session between a mobile station and the base station. Each session belongs to a state of the FSM and each message of the session is compared to the possible messages allowed in such state to verify the validity of the message. Details of this component are explained in the next subsection.

Finite state machine: The proposed intrusion detection system employs a Finite State Machine (FSM) for detecting malicious messages in the PKMv2 EAP-AKA authentication process (Fig. 3). Nodes represents the state of the session between a mobile station and the base station and edges represents the possible correct messages that the mobile station or base station can transmit in each state. Description of each state is described in Table 1. From here, the prefix “PKMv2 EAP-Transfer” in each EAP-Transfer message is omitted.

The FSM specifies the possible message flows in a communication session between a mobile station and the base station during the PKMv2 EAP-AKA authentication and uses it to identify malicious messages. Malicious messages are easily detected because they violate the normal state transition of FSM. Pseudocode 3 below shows part of its functionality.

Pseudocode 3: Finite State Machine

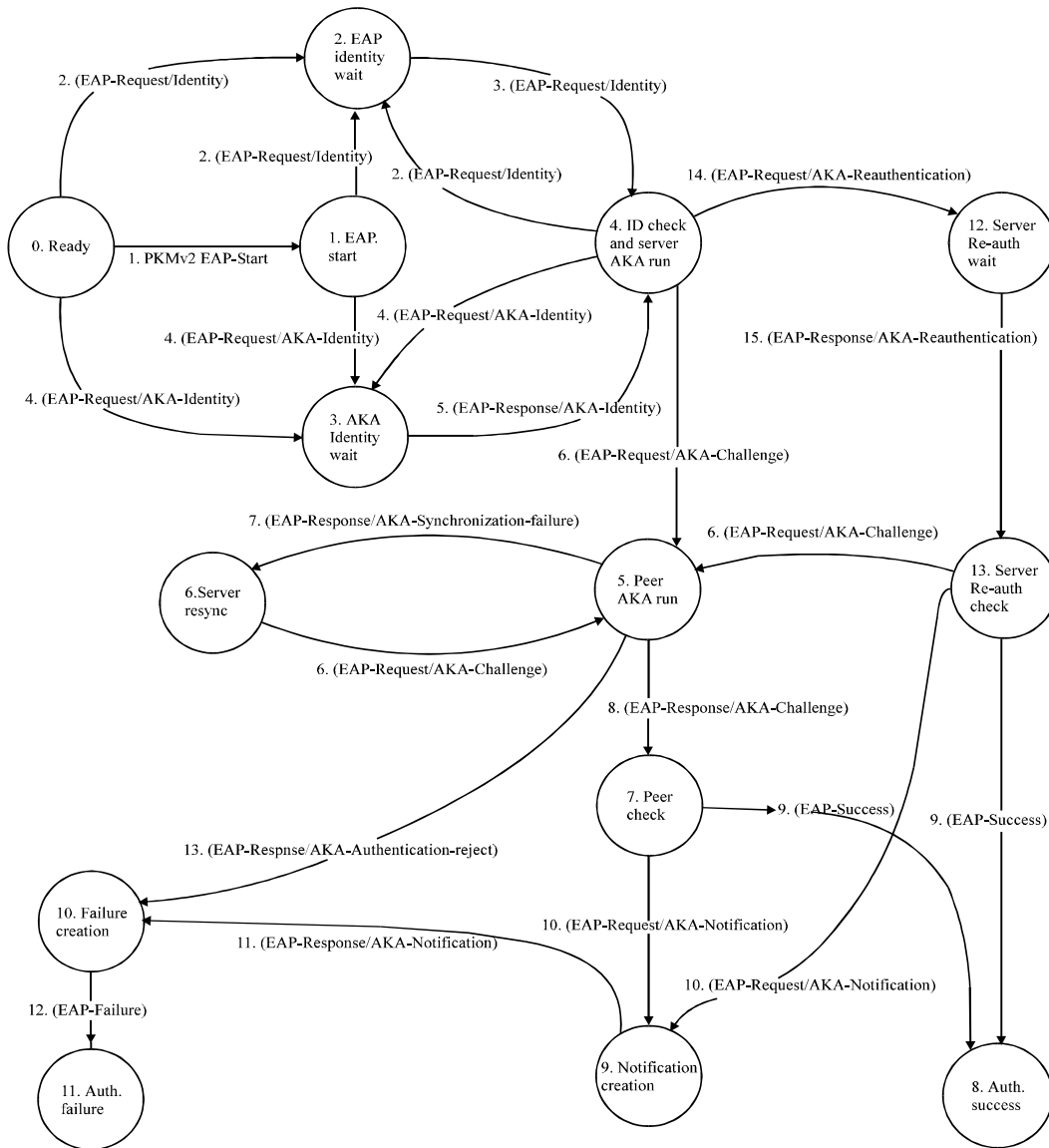
```
function bool finite_state_machine (state CID_state, message M) {
  switch (CID_state) {
    case 0:
      if ((M.type==1) || (M.type==2) || (M.type==4))
        return true;
      break;
    case 1:
      if ((M.type==2) || (M.type==4))
        return true;
      break;
    ...
  }
  if Is_Error_Case(CID_state, M)
    return true;
  return false;
}
```

As example of FSM usage, below is the description of how attacks mentioned in ‘Vulnerabilities in WiBro’ are detected by the proposed FSM.

- Denial of Service attack based on EAP-Failure message: the system transmits an alarm message to the base station when a (EAP-Failure) message is transmitted in a different state than state 10 of Fig. 3 (See also error cases section below)
- EAP-Failure inducing Denial of Service attack: the system transmits an alarm message to the base station when a (EAP-Response/AKA-Authentication-Reject) message is transmitted in a different state than state 5 or when (EAP-Response/AKA-Notification) message is transmitted

Table 1: States of finite state machine

State	Description
0. Ready	Initial state waiting for new authentication sessions.
1. EAP-start	State after mobile station has sent the PKMv2 EAP-Start message to request authentication process to the base station.
2. EAP Identity wait	State after base station has sent the (EAP-Request/Identity) message and waits for the (EAP-Response/Identity) message.
3. AKA: Identity wait	State after base station has sent the (EAP-Request/AKA-Identity) message and waits for the (EAP-Response/AKA-Identity) message.
4. ID check and server AKA run	State when the base station receives (EAP-Request/Identity) or (EAP-Request/AKA-Identity) message and verifies the received message to decide if request another authentication message (fast re-authentication or another identity) or run AKA algorithms to generate RAND and AUTN.
5. Peer AKA RUN	State when mobile station receives (EAP-Request/AKA-Challenge) message. In this state, the mobile station can request the re-synchronization to the base station or run AKA algorithm to verify the AUTN and MAC values received from base station.
6. Server resync	State when base station receives (EAP-Response/AKA-Synchronization-Failure) message sent by the mobile station. In this state, the base station sends (EAP-Request/AKA-Challenge) again after synchronization.
7. Server checks peer	State when base station receives (EAP-Response/AKA-Challenge) message. In this state the authentication server verifies the RES and MAC values to allow or deny access to WiBro.
8. Authentication success	State when the mobile station receives (EAP-Success) message indicating a successful authentication.
9. Notification creation	State when the mobile station receives (EAP-Request/AKA-Notification) because the server found RES or MAC incorrect
10. Failure creation	State when the base station receives (EAP-Response/AKA-Notification) from the mobile station
11. Authentication failure	State when the mobile station receives (EAP-Failure) message from the base station indicating that the authentication process has failed.
12. Server re-authentication wait	State when the mobile station receives the (EAP-Request/AKA-Reauthentication) message. In this state, the base station waits for the (EAP-Response/AKA-Reauthentication) message.
13. Server re-auth check	State when the base station receives the (EAP-Response/AKA-Reauthentication) message. In this state, the server verifies the validity of reauthentication values and responds with a (EAP-Success) message (EAP-Request/AKA-Notification) message or (EAP-Request/AKA-Challenge) message if they are valid, invalid or if full authentication is required, respectively.



Note: Prefix PKMv2 EAP-transfer was omitted in every message except the message 1

Fig. 3: Finite state machine

in a different state than 9 or when (EAP-Response/AKA-Client-Error) message is transmitted before a correct message

- Denial of Service attack based on PKMv2 EAP-Start messages: the system generates an EAP-Start alarm when it detects more PKMv2 EAP-Start message transmissions with the same CID than the threshold value
- RES-CMD Replay Attack: the system generates a RES-CMD alarm when RES-CMD transmissions exceed the threshold value. This attack is hard to be

detected if the attacker sends a RES-CMD message to a different mobile station and uses long interval of time in each attack

- RES-CMD induction attack based on replay: the system generates a RES-CMD alarm when: (1) the (EAP-Response/Identity) or (EAP-Response/AKA-Identity) message transmissions in state 2 or 3 exceed the threshold value (2) the (EAP-Response/AKA-Challenge) message transmissions in state 5 exceed the threshold value or (3) the (EAP-Response/AKA-Notification) message transmissions in state 9 exceed

the threshold value; or (4) the (EAP-Response/AKA-Reauthentication) message transmissions in state 12 exceed the threshold value

- Flooding attack in EAP-AKA authentication process: the system generates a Flooding alarm when it detects more than a threshold number of EAP messages violating state transitions
- Resynchronization looping denial of service attack: the system generates a Resynchronization looping alarm when it detects more than a threshold number of (EAP-Response/AKA-Synchronization-Failure) messages in state 5

Error cases control: The specification of EAP-AKA (Arkko and Haverinen, 2006) also describes the error cases that may occur in EAP-AKA. Some of such error cases were not defined in the proposed FSM to keep its simplicity. This section gives details of the mentioned error cases and how the proposed system manages them.

- **Peer operation error case:** when a mobile station detects an error in a received EAP-AKA message, the mobile station responds with the (EAP-Response/AKA-Client-Error) message. In response to the (EAP-Response/AKA-Client-Error), the EAP server must issue the (EAP-Failure) message and the authentication exchange terminates

Solution: If (EAP-Response/AKA-Client-Error) message is detected, the intrusion detection system waits for a period of time for other valid message coming from the mobile station with same CID. If no other valid message of the session is detected, the session is reset; otherwise, the intrusion detection system generates an intrusion alarm. Depending how base station is configured the session may remain and execute the normal state transition.

- **Server operation error case:** when the base station issues an (EAP-Request/AKA-Notification) that implies failure which includes the following: (1) the server is not able to parse the mobile station's EAP response (2) the server encounters a malformed attribute, a non-recognized non-skippable attribute or a duplicate attribute (3) a mandatory attribute is missing or an invalid attribute was included (4) unrecognized or unexpected EAP-AKA subtype is in the EAP Response (5) invalid AT_MAC is found (6) invalid AT_CHECKCODE is found or (7) invalid AT_COUNTER is found

Solution: The (EAP-Response/AKA-Notification) only can be transmitted just after a message transmission from

the mobile station; therefore (EAP-Response/AKA-Notification) message is accepted, only if it is transmitted in states 1, 4, 6, 7, 10 or 13. Additionally, if (EAP-Response/AKA-Notification) message is detected, the intrusion detection system waits for a period of time for other valid message coming from the base station with same CID. If no other valid message of the session is detected, the session is reset; otherwise, the session generates an intrusion alarm.

- **EAP-failure error case:** The EAP-AKA server sends (EAP-Failure) in three sub-cases: (1) in response to an (EAP-Response/AKA-Client-Error) message or (2) in response to an (EAP-Response/AKA-Authentication-Reject) message or (3) following an EAP-AKA notification round when the AT_NOTIFICATION code implies failure

Solution: In this error case, only the first sub-case is not managed by the FSM. To manage this sub-case, the intrusion detection system verifies that the (EAP-Failure) message is coming just after the (EAP-Response/AKA-Client-Error) message; otherwise the system generates an intrusion alarm.

The specification of EAP-AKA also describes error case related with EAP-Success. However, such case is not detailed in this section because their management was already included in the FSM.

IMPLEMENTATION AND SIMULATION

To demonstrate the feasibility of implementation in a real environment, an experimental network was implemented. The experimental environment, shown in Fig. 4, is comprised of mobile stations, RSA/ACR (Radio Access Station/Access Control Router), Attacker, the Intrusion Detection System and AAA (Authentication, Authorization and Accounting) Server. The WiBro security sublayer of mobile stations was developed with features based on the WiBro standard and RFC4187. RAS/ACR was emulated by using an Access Point (AP) that supports 802.1X with wireless message reception role (RAS) and EAP messages transmission role (ACR). The AAA server was implemented using a RADIUS server including EAP-AKA features. The attacker was implemented using C# to sniff the wireless channel and capture the plaintext data and insert malicious messages. Finally, the intrusion detection system was implemented using C#. The CID was simulated by the combination of mobile station and base station IP addresses.

Figure 5 illustrates the main screen of the intrusion detection system which comprises of four sections:

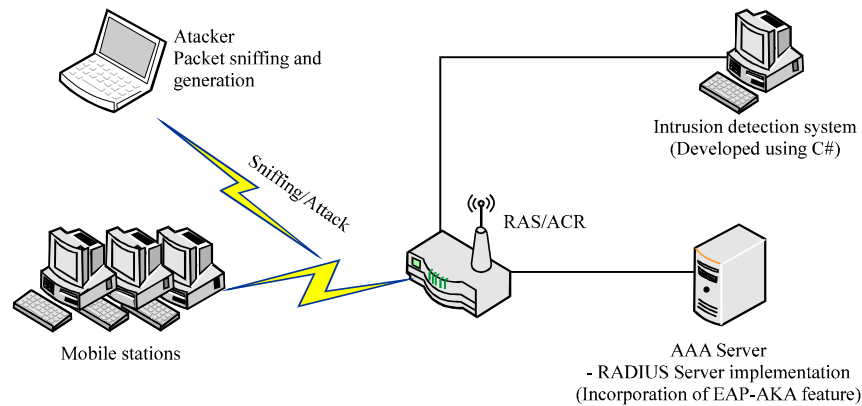


Fig. 4: Simulation environment

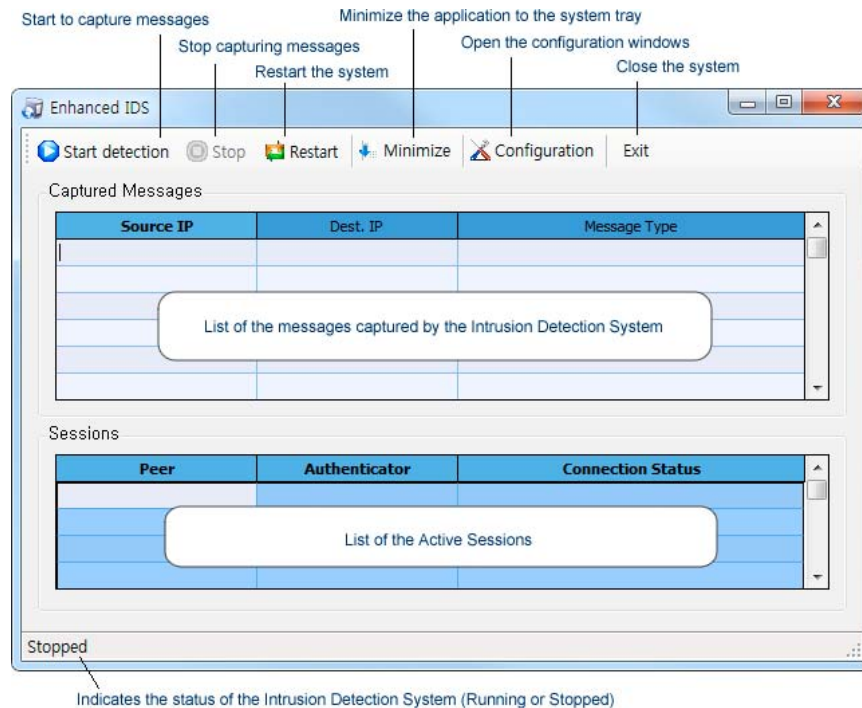


Fig. 5: Main screen of the intrusion detection system

(1) menu bar containing the buttons which activates features of the system (2) list of captured PKMv2 EAP-AKA messages (3) list of sessions between mobile stations and base station and (4) status bar which indicates the status of the system.

Several simulations scenarios including the normal state transition of the FSM as well as attack scenarios that violates the normal state transition of the FSM were executed.

Normal flow scenarios and results: Six scenarios simulating the normal flow of the FSM were executed, including a successful authentication, successful authentication with resynchronization, failed authentication and so on. Below are explained the simulation scenarios and their results.

Scenario 1: (Successful authentication): the typical valid authentication flow was executed in this scenario. This

scenario includes the following state sequence: 0→1(optional)→2(or 3)→4→5→7→8.

Scenario 2: (Successful authentication with server resynchronization): this scenario executes the scenario 1 plus the server resynchronization process. This scenario includes the following state sequence: 0→1(optional)→2(or 3)→4→5→6→5→7→8.

Scenario 3: (Failed authentication): the typical failed authentication flow was executed in this scenario. This scenario includes the following state sequence: 0→1(optional)→2(or 3)→4→5→7→9→10→11.

Scenario 4: (Successful fast re-authentication): the typical valid fast re-authentication flow was executed in this scenario. This scenario includes the following state sequence: 0→1(optional)→2(or 3)→4→12→13→8.

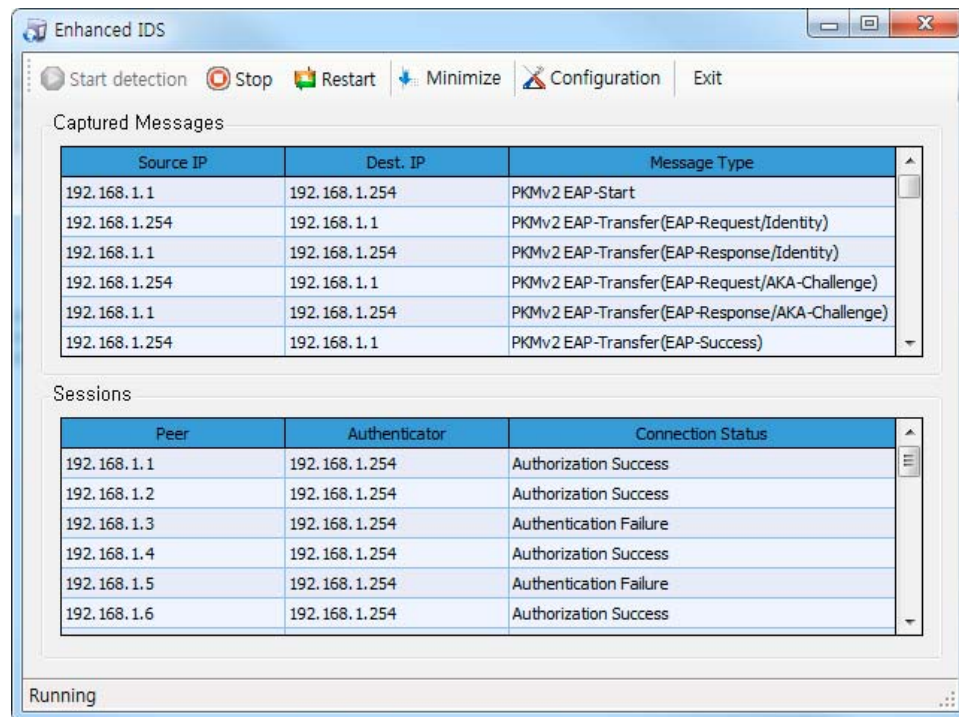
Scenario 5: (Failed fast re-authentication): the typical invalid fast re-authentication flow was executed. This scenario includes the following state sequence: 0→1(optional)→2(or 3)→4→12→13→9→10→11.

Scenario 6: (Transition from fast re-authentication to full authentication): this scenario executes the typical transition from the fast re-authentication process to the full authentication process. This scenario includes the following state sequence: 0→1(optional)→2(or 3)→4→12→13→5→7→8.

Figure 6 illustrates the screen of the Intrusion Detection System monitoring the concurrent execution of six scenarios described above. The mentioned figure shows the source and destination addresses and message type of captured messages; the figure also indicates the communication sessions and their final state.

Attack scenarios and results: Attacks detailed in Vulnerabilities in WiBro (Security in WiBro) were also simulated to verify the intrusion detection capabilities of the proposed solution. Below are explained the attack scenarios and their results.

Scenario 1: the attacker uses a spoofed base station to send (EAP-Failure) messages to the mobile station. Figure 7 illustrates how the proposed system detects this attack.



The screenshot shows the 'Enhanced IDS' window with a toolbar containing 'Start detection', 'Stop', 'Restart', 'Minimize', 'Configuration', and 'Exit'. Below the toolbar, there are two main sections: 'Captured Messages' and 'Sessions'.

Captured Messages Table:

Source IP	Dest. IP	Message Type
192.168.1.1	192.168.1.254	PKMv2 EAP-Start
192.168.1.254	192.168.1.1	PKMv2 EAP-Transfer(EAP-Request/Identity)
192.168.1.1	192.168.1.254	PKMv2 EAP-Transfer(EAP-Response/Identity)
192.168.1.254	192.168.1.1	PKMv2 EAP-Transfer(EAP-Request/AKA-Challenge)
192.168.1.1	192.168.1.254	PKMv2 EAP-Transfer(EAP-Response/AKA-Challenge)
192.168.1.254	192.168.1.1	PKMv2 EAP-Transfer(EAP-Success)

Sessions Table:

Peer	Authenticator	Connection Status
192.168.1.1	192.168.1.254	Authorization Success
192.168.1.2	192.168.1.254	Authorization Success
192.168.1.3	192.168.1.254	Authentication Failure
192.168.1.4	192.168.1.254	Authorization Success
192.168.1.5	192.168.1.254	Authentication Failure
192.168.1.6	192.168.1.254	Authorization Success

At the bottom of the window, the status 'Running' is displayed.

Fig. 6: Concurrent execution of normal flow scenarios

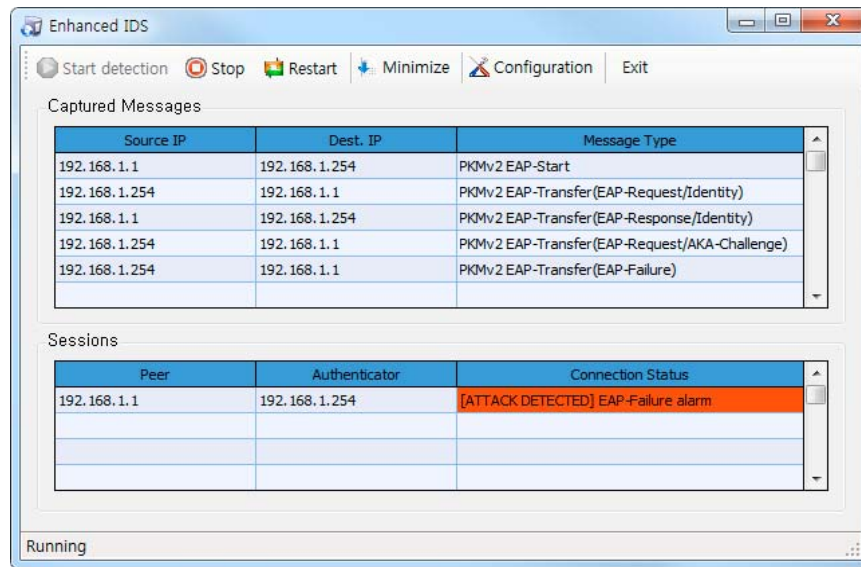


Fig. 7: Detection of the DoS attack based on EAP-failure messages

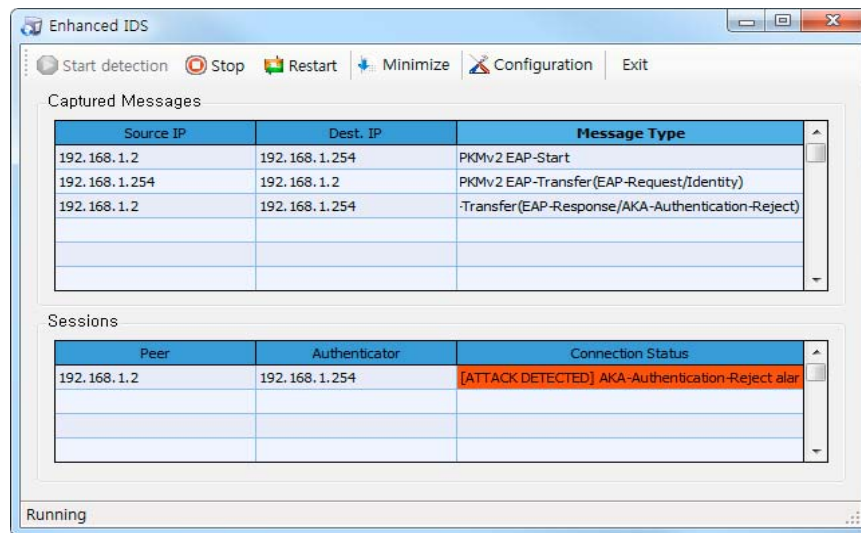


Fig. 8: Detection of the EAP-failure inducing DoS attack

Scenario 2: During the authentication process, the attacker using a spoofed mobile station sends an (EAP-Response/Challenge-AKA-Authentication-Reject) message to the base station to provoke an (Challenge-AKA-Authentication-Reject). Figure 8 illustrates how the proposed system detects this attack.

Scenario 3: The attacker obtains the Identity and CID from an authentication process and sends several PKMv2

EAP-Start messages to the base station. Figure 9 illustrates how the proposed system detects this attack.

Scenario 4: During the authentication process, the attacker using a spoofed base station sends several RES-CMD messages to the mobile station. Figure 10 illustrates how the proposed system detects this attack.

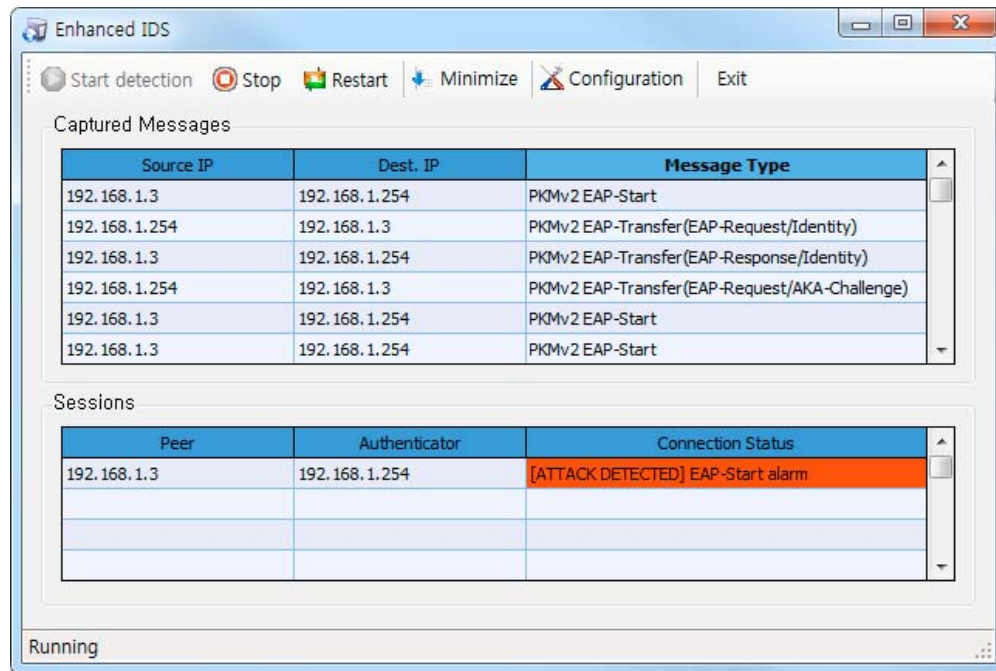


Fig. 9: Detection of DoS attack based on PKMv2 EAP-start messages

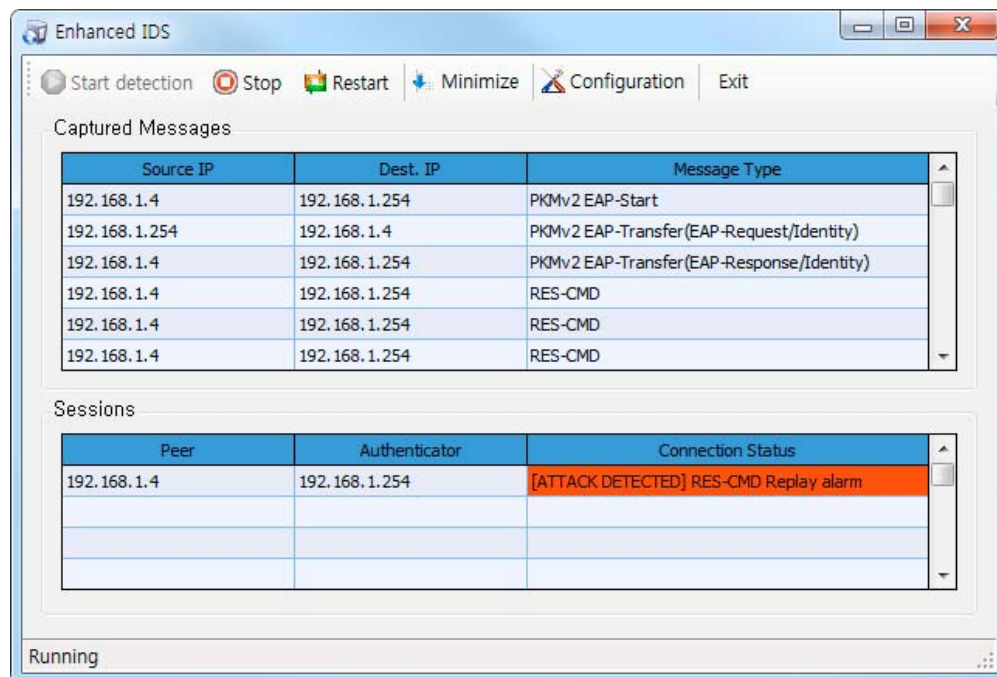


Fig. 10: Detection of RES-CMD replay attack

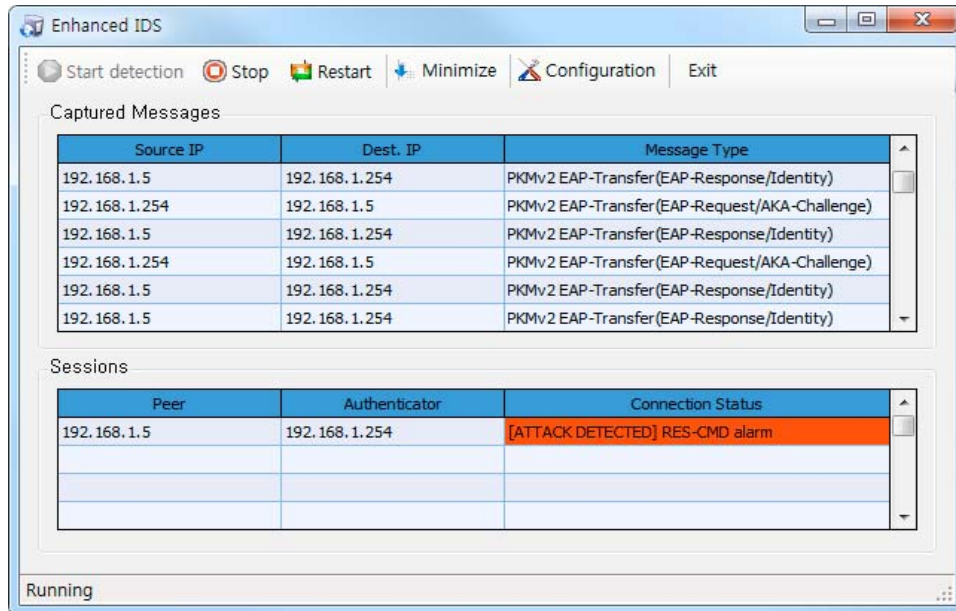


Fig. 11: Detection of RES-CMD induction attack based on replay

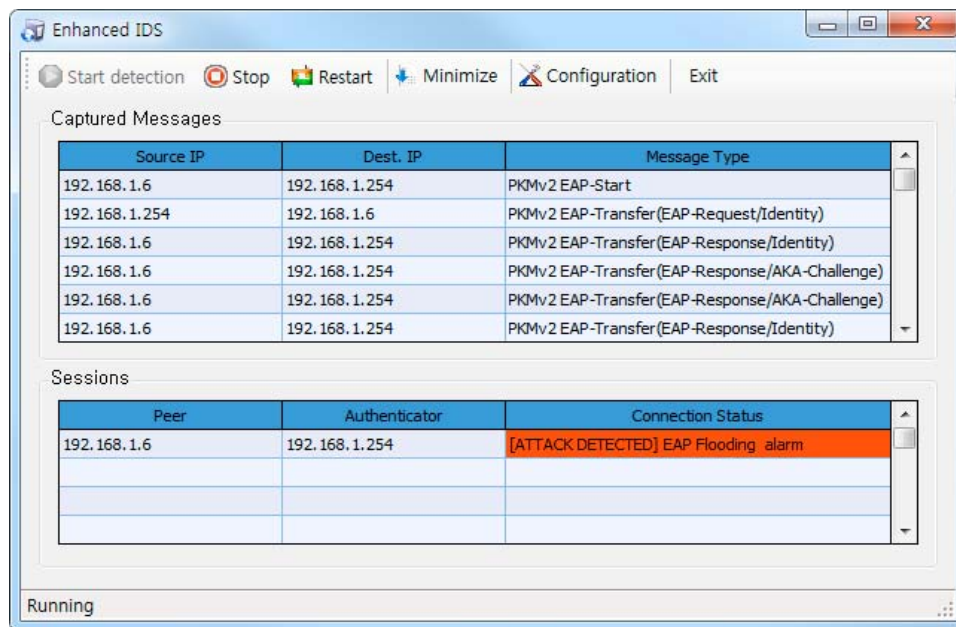


Fig. 12: Detection of EAP flooding attack

Scenario 5: During the authentication process, the attacker sends several (EAP-Response/Identity) messages to base station. Figure 11 illustrates how the proposed system detects the attack executed in this scenario.

Scenario 6: The attacker, by using a spoofed mobile station, continuously sends several random EAP messages. Figure 12 illustrates how the proposed system detects the attack executed in this scenario.

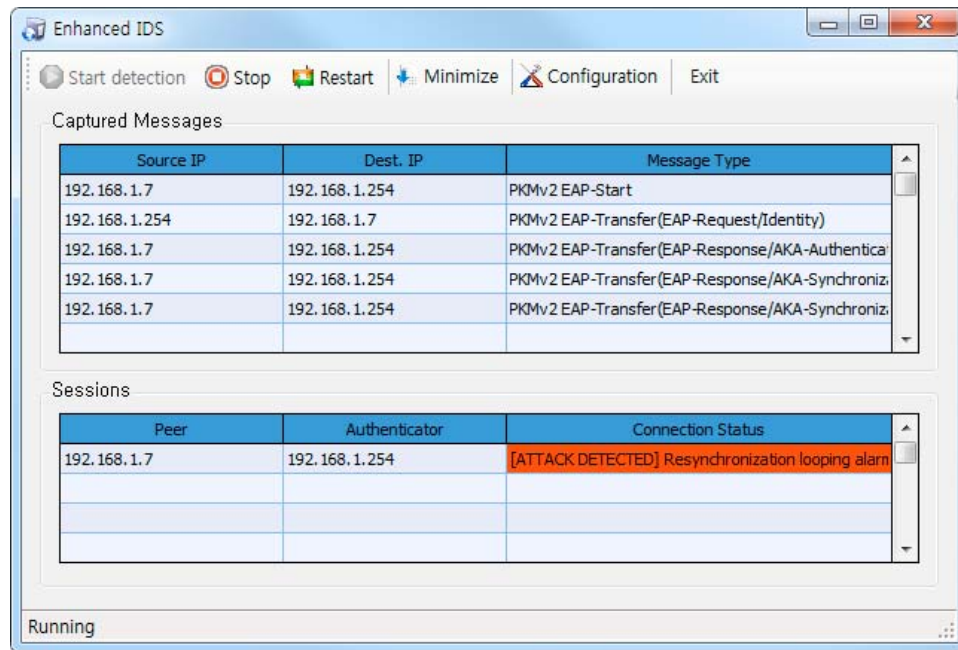


Fig. 13: Detection of resynchronization looping DoS attack

Scenario 7: The attacker, by using a spoofed mobile station, sends continuously several (EAP-Response/AKA-Synchronization-Failure) messages. Figure 13 illustrates how the proposed system detects the attack executed in this scenario.

CONCLUSION

Present study has proposed an enhanced specification-based intrusion detection system for WiBro which detects effectively malicious attacks executed in the initial authentication phase. The proposal provides a complete specification of the normal flow of PKMv2 EAP-AKA including the fast re-authentication process and error cases. To demonstrate the feasibility of the proposed solution in a real environment, an experimental network was implemented which includes an intrusion detection system developed in C# with a user friendly visual interface and concurrent session management capabilities. The intrusion detection abilities of the system were tested by executing a variety of simulations. The specification-based characteristic of the intrusion detection system allows effective detection of unknown attacks which is very useful in a complicated WiBro environment with the potential to be a victim of new type of attacks in the future.

REFERENCES

- Altaf, A., M.Y. Javed and A. Ahmed, 2008. Security enhancements for privacy and key management protocol in IEEE 802.16e-2005. Proceedings of the 9th ACIS International Conference of Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Aug. 6-8, IEEE., pp: 335-339.
- Anderson, D., T. Lunt, H. Javitz, A. Tamaru and A. Valdes, 1995. Next-generation Intrusion Detection Expert System (NIDES): A summary. SRI-CSL-95-07, SRI International.
- Arkko, J. and H. Haverinen, 2006. Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA). RFC4187, <http://tools.ietf.org/html/rfc4187>.
- Bahaman, N., A.S. Prabuwo and M.Z. Masud, 2011. Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism. J. Applied Sci., 11: 118-124.
- Bhargava, B., Y. Zhang, N. Idika, L. Lilien and M. Azami, 2009. Collaborative attacks in WiMAX networks. Security Communicat. Networks, 2: 373-391.
- Ei, T. and W. Furong, 2010. Trajectory-aware vertical handoff protocol between WiMAX and 3GPP networks. Inform. Technol. J., 9: 201-214.

- Eshanta, O.M., M. Ismail, K. Jumari and P. Yahaya, 2009. VHO strategy for QoS-provisioning in the WiMAX/WLAN interworking system. *Asian J. Applied Sci.*, 2: 511-520.
- Forrest, S., S.A. Hofmeyr and A. Somayaji, 1997. Computer immunology. *Comm. ACM.*, 40: 88-96.
- Ghosh, A.K., A. Schwartzbard and M. Schatz, 1999. Learning program behavior profiles for intrusion detection. *Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, April 9-12, USA., pp: 51-62.
- Gill, R., J. Smith and A. Clark, 2006. Specification-based intrusion detection in WLANs. *Proceedings of the 22nd Annual Computer Security Application Conference*, December 2006, USA., pp: 141-152.
- IEEE, 2005. IEEE Std 802.16e-2005. IEEE Computer Society and the IEEE Microwave Theory and Techniques Society.
- Jha, S., R. Sommer and C. Kreibich, 2010. *Toward Specification-based Intrusion Detection for Web Applications*. Vol. 6307, Springer-Verlag, Berlin, Heidelberg, New York, ISBN: 3-642-15511-1 978-3-642-15511-6, pp: 518.
- Ko, C., P. Brutch and J. Rowe, 2001. System health and intrusion monitoring using a hierarchy of constraints. *Proceedings of the 4th Symposium on Recent Advances in Intrusion Detection*, Oct. 10-12, Davis, CA., pp: 37-53.
- Kumar, S. and E. Spafford, 1994. A pattern-matching model for intrusion detection. *Proceeding of the 17th National Computer Security Conference*, October 1994, Baltimore, pp: 11-21.
- Lee, S.Q., N. Park, C. Cho, H. Lee and S. Ryu, 2006. The wireless broadband (WiBro) system for broadband wireless internet services. *IEEE Comm. Magazine*, 44: 106-112.
- Lee, Y. and S. Lee, 2010. Specification-based intrusion detection system for the initial authentication phase of WiBro. *J. Korea Instit. Inform. Security Cryptol.*, 20: 3-163.
- Malekzadeh, M., A. Ghani, J. Desa and S. Subramaniam, 2009. Vulnerability analysis of Extensible Authentication Protocol (EAP) DoS attack over wireless networks. *ICGST-CNIR J.*, 9: 39-46.
- Porras, P.A. and R.A. Kemmerer, 1992. Penetration state transition analysis: A rule based intrusion detection approach. *Proceedings of the 8th Annual Computer Security Applications Conference*, Nov. 30-Dec. 4, USA., pp: 220-229.
- Raja, P.C.K., M. Suganthi and R. Sunder, 2008. Wireless node misbehavior detection using genetic algorithm. *Inform. Technol. J.*, 7: 143-148.
- Sakib, A.K.M.N., M.I. Khan and M.M.S. Kowsar, 2010. IEEE 802.16e security vulnerability: Analysis and solution. *Global J. Comput. Sci. Technol.* Vol. 10,
- Sekar, R., A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang and S. Zhou, 2002. Specification based anomaly detection: A new approach for detecting network intrusions. *Proceedings of the 9th ACM Conference on Computer and Communications Security*, Nov. 18-22, Washington, DC, USA., pp: 265-274.
- Shahid, M.K., T. Shoulain and A. Shan, 2008. Mobile broadband: Comparison of mobile WiMAX and cellular 3G/3G+ technologies. *Inform. Technol. J.*, 7: 570-579.
- TTA, 2005. Specifications for 2.3GHz band portable internet (WiBro) service. Physical and Medium Access Control Layer. TTA Standard TTAS.KO-06.0082.
- TTA, 2006. Specifications for mutual authentication mechanism for 2.3GHz band portable internet (WiBro) service. TTA Standard TTAS.KO-06.0110/R1.
- TTA, 2007. TTA: WiBro overview. Telecommunications Technology Association, <http://www.wibro.or.kr>.
- Tseng, C.Y., C. Ko, R. Limprasittipom, J. Rowe and K. Levitt, 2003. A specification-based intrusion detection system for AODV. *Proceedings of the 1st ACM Workshop on Security of ad-hoc and Sensor Networks*, Oct. 27-30, USA., pp: 125-134.
- Tseng, C.H., T. Song, P. Balasubramanyam, C. Ko and K. Levitt, 2006. A specification-based intrusion detection model for olsr. *Lecture Notes Comput. Sci.*, 3858: 330-350.
- Wu, C.F., 2010. Real-time scheduling for multimedia services in IEEE 802.16 wireless metropolitan area network. *Inform. Technol. J.*, 92: 1053-1067.