AiMT

Advances in Military Technology
Vol. 14, No. 2 **(2019)**, pp. 331-346
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01289

# Sleeping Encryption Unit in the Integrated Air Defence Systems

O.A. Dawood[1]*, H. Almulla[1] and S. Khan[2]

[1] *College of Computer Sciences and Information Technology, University Of Anbar, Anbar, Iraq*
[2] *Department of Computer and Information Sciences, Northumbria University, Newcastle, UK*

The manuscript was received on 31 January 2019 and was accepted after revision for publication on 10 November 2019.

**Abstract:**

*This research introduces a new military crypto-cipher authentication model developed for an Integrated Air Defence System (IADS). This study focused on the encryption aspect that is built as a hidden cryptographic of a sleeping encryption unit (SEU) in an IADS. SEU is utilised as a sleeping unit under the control of manufacturer countries during wartime. SEU permits high access to manufacturer countries to remotely deactivate an IADS. This hidden unit identifies and verifies targets before targeting them, thereby preventing their destruction at a critical time. Algorithms and protocols assigned to this unit are often confidential, highly secret and undisclosed.*

**Keywords:**

*crisis management, integrated air defence system (IADS), military mobility, Patriot PAC-3 usa, S-400 & S-500*

## 1. Introduction

Mobility, speed and flexibility are the triple pillars that an integrated air defence system (IADS) must satisfy. Current IADS systems have progressed substantially in recent years to face new types of threats and perform considerably dynamic tasks [1]. The reason for this circumstance is that every country seeks to arm itself with the latest equipment and sophisticated weapons to secure its borders and sovereignty against any threat and aggression [2]. Note that developed countries that have the best IADS are Russia and the US. Particularly, Russia has a highly advanced IADS that can hit targets from a considerable distance. IADS involves anti-early warning aircraft, jam-

* *Omar A. Dawood, Computer Science Department, University of Anbar, Anbar City, Iraq. Phone: +964 79 05 88 43 33, E-mail: the_lionofclub@yahoo.com, Omar-Abdulrahman@uoanbar.edu.iq. ORCID 0000-0003-3276-602X.*

ming planes, reconnaissance aircraft and short-, medium- and long-range anti-ballistic missiles [3]. The source model contains a hidden 'brake' unit that prevents the use of this weapon against its maker, called sleeping encryption unit (SEU) or interrogator unit. This secret unit could be a beacon operating during a war under the control of the manufacturer country. SEU may also be a special button run remotely or an 'encryption program' meant to be 'asleep' or 'idle' at all times. In case of war with the manufacturer country, SEU will remain active and will not produce an accurate report against the original manufacturer country [4]. When manufacturers or technology-exporting countries sell a new IADS, they traditionally do not disclose the encryption secret unit in the system. The majority of the countries importing this technology are attempting to develop similar versions of the original imported version. However, production of copies of precision weapons ultimately fails to generate the same product because of the low quality and undesirable characteristics of the reproductions [5].

Modern IADS involves integrated system missiles designed to hit aerodynamic targets of tactical and strategic air-to-air aircraft, Airborne Warning and Control System (AWACS) and winged missile systems. Such IADS also intersects ballistic missiles, ultrasonic targets and many state-of-the-art and future air attack modes with absolute precision. The majority of developed countries that produce missile defence systems retain many of the hidden internal techniques of the system. During the delivery of these systems to the concerned party, such techniques will be either in its amended form or in a modified technology that is undisclosed [6]. The delivered system in the modified version is considered part of the secret production of the industrialised countries. These secrets cannot be given completely to any importing country because they are regarded as industrial secrets. These secret techniques are the results of the accumulated experience of thousands of scientists over the years [7]. This paper will discuss the ways of designing and operating an encryption module in IADS and establishing a developed applicable cryptosystem.

## 2. Functions of IADS

IADS is an integrated system that consists of three essential components: intelligent software, advanced hardware and trained specialists. The air defence battery involves several interconnected units aggregated into an integrated and complete intelligent system. The main objective of IADS is to provide an advanced technology for monitoring, detecting, identifying, intercepting and tracking missile path and hitting targets with high accuracy. Moreover, IADS can be used to destroy and intercept the threats of hostile missiles. The main components of this system are embedded and collected devices, which include a communications mode, command and fire controller, radar surveillance device, missile director and missile launcher as stated in Fig. 1 [8, 9].

The components of IADS combine to function in a coordinated and integrated mode. The fundamental role of the communications mode is to support reliability and integrity with real-time broadcasting information. Moreover, the communication mode ensures online connection to the distanced system batteries through steady communication, even if the system is exposed to radio interference [10]. The command and fire control unit is responsible for setting up a real communication system that is compatible with several sensor systems. The radar surveillance device is the primary unit in the air defence battery that facilitates scanning with different bands of radio frequen-

cies for the encrypted wavelengths. The scanning process occurs in different directions for the immediate discovery of objects.

Thereafter, the radar will detect the ranges, angles, sizes and speed of targets. If the target is near the critical zone, then the radar will submit a reported 'image' of the target to the control unit. The report will be sent across long distances to acquire an immediate radar signature that is issued after intelligent investigation and analysis from a quick reported image. The radar will accurately identify the targeted nature in the sky or at sea. Subsequently, the radar immediately detects the incoming threat for a real-time response [11, 12]. The missile director unit tracks unfriendly targets and directs the warhead of different types of missiles to proactively determine threatening goals. The last IADS component is the missile launcher platform that receives the final instruction from the cockpit to launch the fire for intercepting and destroying targets with high speed and accuracy using smart guided missiles as illustrated in Fig. 2. The entire operation entails a maximum of under one minute [13].

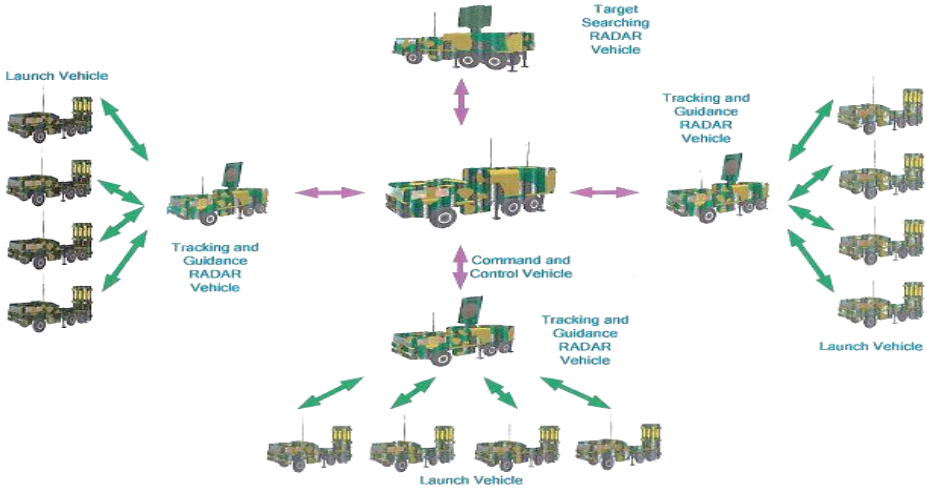


*Fig. 1 IADS Model*

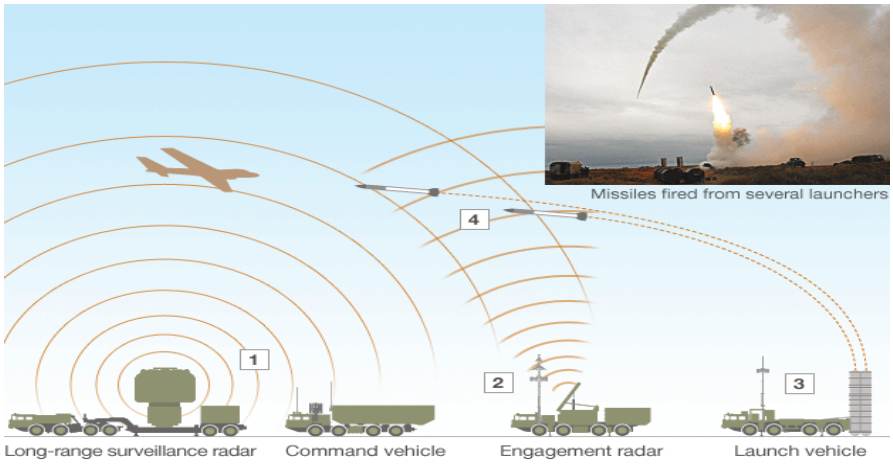


*Fig. 2 Air defence battery launching target*

All IADS components use typical intelligent weapons, sensors, and command and control instruments prepared to cover the tactical scenario. The following list presents the best IADS in the world [14]:

1. S-500: Russia
2. S-400: Russia
3. THAAD: US
4. Antey-2500-S-300V4: Russia
5. Meads: US
6. S-300 PMU2: Russia
7. SAMP/T: France, Italy
8. Patriot PAC-3: US
9. HQ-9: China
10. Barak-8: Israel, India
11. S-350 Vityaz: Russia
12. Shu-SAM: Japan
13. Akash: India
14. Flakpanzer Gepard: Germany
15. Sky Sabre: UK
16. AN/FPS-120 radar: Denmark
17. AN/FPS-129 radar: Norway
18. M3R radar: The Netherlands
19. PAAMS: Italy
20. Mobile AN/TPY-2 radar: Turkey
21. SM-3: Romania
22. Sea-based Aegis System Planned: Spain
23. Arrow missiles: Israel
24. AN/TPY-2: South Korea
25. AN/SPQ-9B: Australia

## 3. SEU or Interrogator Unit

An SEU or interrogator unit is a hidden unit whose location most manufacturing companies avoid disclosing along with their function in the majority of modern IADS [15]. SEU encrypts the transmitted radio waves and sends the encrypted messages with high-frequency signals for long distances. When the signals collide with the target object, IADS will analyse and identify the targeted nature as being friendly or hostile. This unit should be pre-embedded to all army, air, land and marine units by the same manufacturer with the same cryptosystem model. Thus, all military units must be equipped with the same cryptosystem to be compatible with each other. An encrypted signal received by the target is analysed immediately by the same cryptosystem to produce a verified signature for IADS to avoid engagement with the authorised target [16]. Consequently, countries that import IADSs will be unable to use this system against the manufacturing countries' targets. The reason is that the exporting country knows the internal secrets of the system and has a full control over it.

Therefore, manufacturing countries should not worry about IADS being used against them during war. Note that the majority of these systems are designed with a brake system that prevents them from colliding with the targets that work with the same coding programs [17]. The main idea behind this unit is to identify friends from enemies in real-time and to prevent the use of this system against the exporting country. SEU consists of several concatenated algorithms that work together with hundreds of equations in embedded dedicated devices with a unified platform. Thus, the majority of the countries that import these systems seek to diversify their imports of IADS from different countries. Importing countries seek to diversify their IADS from multi-states so as not to be hostage to a single manufacturer's state if war breaks out between them. The reason is that the importing countries of IADS are unable to use them against the exporting countries. Furthermore, the secrets of this system from the manufacturer countries may be sold to hostile countries without the knowledge of the importing countries, thereby leading to an imbalance in power between states [18]. However, the system will be subject to a complete control by exporting countries at any time. These circumstances are the major reasons why most countries do not rely

on one type of IADS. The majority of countries attempt to be self-reliant in manufacturing their own IADS and endeavour to diversify their systems from multi-resources [19].

## 4. Proposed SEU

This study will simulate a proposed cryptosystem for the design of a new SEU with its encryption algorithm primitives. The proposed model consists of several combined symmetric block ciphers that work on one platform with hundreds of linear and non-linear equations. The developed model involves only four main phases: S-boxes, shifting, linear MDS and key generation phases. Each phase with multi-stages is recursively repeated for several predetermined rounds. The selection of the algorithm phase is determined through the connection session, in which each phase involves hundreds of choices for the selected operation. The first phase is responsible for the confusion property and consists of 300 different S-boxes with their inverses.

The proposed S-Boxes work with different affine and irreducible equations generated by several mathematical techniques. These S-boxes are numbered or indexed from 1 to 300 in addition to indexing their inverses. The second phase of the proposed system is responsible for the diffusion property of this model. This phase includes 100 distinct indexed shifting and rotations processes for various state matrices with different dimensions along with the indexing of their inverses. The third phase of the proposed model also contains over 100 various indexed linear equations. The proposed equations are indexed with the different dimensions used for the mixing layer and with their inverses. The last phase in this system comprises the key generation centre, which involves several techniques of key scheduling methods and generates strong secret keys with different lengths.

The generated ciphering keys are stored in a secret directory. The selected stage in each phase through the encryption process is initiated from the radar side. Additionally, all information of the four phases, which includes the stage indexing number, is also manually or automatically selected by the radar. Thereafter, the radar will send the indexing number of each selected stage in the system with the encrypted message to the target. The target will receive the encrypted authentication message and the indexing number for the selected stages in the system. The indexing number will assist the target in decrypting the encrypted message on the basis of the selected stages through which they are encrypted.

## 5. Main Design Objective

Although the majority of the details of this research favour military applications, the core idea of the study involves cryptography. The main purpose of this security system is to design IADS that is applicable for military utilisation, particularly to protect borders against external threats. The first purpose of the proposed system is to identify and verify the targets remotely by depending on the proposed SEU installed in IADS. The proposed secret unit must be installed in all systems of various army, marine and air defence units. SEUs must be compatible in a holistic manner with one another by using the same system and can be clearly identified in cases of clashes. The proposed cryptosystem model is embedded in the SEU unit to readily obtain verification from unknown targets. The verification session is performed by establishing a secure handshaking procedure. If the enemy knows the secrets of the internal operations and

mathematical foundation of SEU, then IADS would be rendered useless. Occasionally, the secrets of SEUs are exclusively sold by the manufacturer countries to other allies without the knowledge of importing countries. The second purpose of SEU is to unify all types of military units in a country by using a standard security system as an authorisation platform. The proposed cryptosystem ensures the authorised access of all authorised parties without affecting the function of the radar in times of peace and war. The manufacturers of these technologies remain completely aware of how to control them for their own interest and how to exert such control even when the technologies are sold and used by another party through a secret backdoor during urgent times.

## 6. System Framework

The main idea behind the proposed system relies on the radar unit that discovers a certain target. The radar establishes the handshaking process with the target on the basis of the handshaking establishment procedure in real time. Thereafter, the radar sends an encrypted message across SEU to the target. The target decrypts the message on behalf of the agreement of handshaking protocols, including message length, ciphering key length and state dimension (see Table 1). The target subsequently re-encrypts the message in reverse order and sends it to the radar, which receives the encrypted message in reverse order from the target. Thereafter, the radar will match the reverse order of the encrypted message with the pre-encrypted message it generated. If the two messages are compatible, then the session will be successful; otherwise, the session will be aborted.

The Handshaking Establishment Protocols:

- **A:** Ciphering message length (128-bit to 2048-bit);
- **B:** Ciphering key lengths of 128, 192, 256, 320, 384, 448, 512, 576, 640, 704, 768, 832, 896, 960 and 1024 or more with multiple of 128-bits;
- **C:** Key generation technique;
- **D:** Ciphering key number for generating a key with specific length;
- **E:** State array dimensions of 4 × 4, 5 × 5, 6 × 6, 7 × 7 or 8 × 8;
- **F:** Non-linear S-box number;
- **G:** Shifting-number with dimensions of 4 × 4, 5 × 5, 6 × 6, 7 × 7 or 8 × 8;
- **H:** Linear mixing of 4 × 4, 5 × 5, 6 × 6, 7 × 7 or 8 × 8 and
- **I:** Number of rounds (10, 20, 30 or more).

The (?) symbol refers to the variable value with a certain range.

*Tab. 1 Packet of Handshaking Agreement Protocols*

| **Protocols** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** |
|---|---|---|---|---|---|---|---|---|---|
| Index. Opr. | **?** | **?** | **?** | **?** | **?** | **?** | **?** | **?** | **?** |
| Indicator | * | * | * | * | * | * | * | * | * |

The packet with the encrypted messages is sent by the radar to the target for verification. Initially, the radar determines the values of cells from the operations indexer in the packet based on the manual or automatic indexing operations. Each number in the packet points to a specific mathematical operation that can be used in the encryption of the message. Thus, the message will be encrypted on the basis of the operation

number in the indexer of operations in the packet. Conversely, the radar will receive the encrypted message accompanied by the packet guide or packet code-book. The target must have the same cryptosystem model similar to the radar to be compatible with the handshaking routine. The system model in the target will automatically decrypt the encrypted message on the basis of the indexer number for each operation and re-encrypts the message in reverse order thereafter and returns it to the radar. When the radar receives the encrypted message from the target, it will decrypt the message on the basis of the same indexer number compared with the decrypted message with a reverse order of the original message. If the two messages are the same, then the verification is accepted; otherwise, the verification is rejected. These operations will take no more than one minute from all sides (radar and targets) at maximum.

**Radar-Side (1):**

- the radar sets up the indexer numbers in the packets with a specific number on the basis of an intended operation index,
- the radar encrypts the message on the basis of the packet indexer setting and
- the radar sends the encrypted message and packet setting to the target.

**Target-Side (2):**

- the target will receive the encrypted message and packet with the setting of indexers' operations as a 'codebook',
- the target will automatically decrypt the message depending on the indexer operation number in the packet using fast processors and
- the target will re-encrypt the message but in reverse order and returns the encrypted message to the radar thereafter.

**Radar-Side (3):**

- the radar receives the encrypted message,
- the radar decrypts the message on the basis of the packet indexer setting,
- the radar compares the decrypted message with the reverse of the original message and
- if the two messages are the same, then the verification is accepted; otherwise, the verification is rejected.

## 7. Possibility of Implementing the Proposed Model for Battlefield Management

The proposed system can be implemented in any simulated platform laptops, servers, super-computers, satellites, WLANs, WWANs and on different wireless networks. The system works as an embedded unit in IADS, which requires extremely fast processing to work in real time during critical events. Some parts of the system are implemented in separate forms as independent published symmetric algorithms, such as the Euphrates cipher [20], Tigris cipher [21] and FAROQ cipher [22] and may be in an extended cipher [23], thereby providing rapid implementation.

The proposed model is considered a package of hundreds of mathematical operations that collectively enable the system to simultaneously handle multi-targets. The proposed cryptosystem is used to maintain the momentum of the battles on the basis of the rules of engagement in difficult times. The command and control centre undertakes the responsibility of management sessions of army and navy units. The coordination occurs with other sub-distributed command and control centres in large areas of the country to protect entire borders. The imposed management information centre re-

quires a suitable terminal crypto-equipment and a convenient host system to cooperate with the external systems and intelligent agencies as shown in Fig. 3 [24].

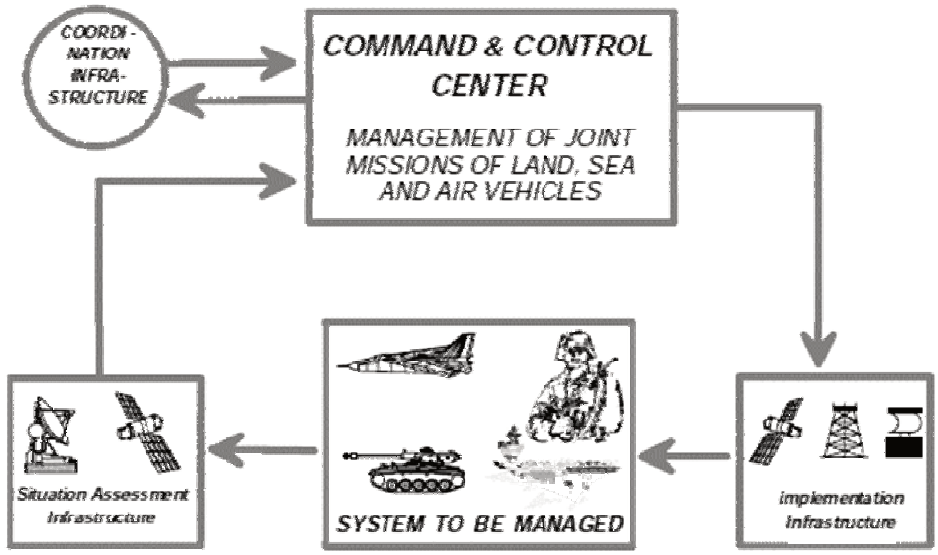


*Fig. 3 Main command and control centre of IADS*

The main characteristics of the command and control cycle loops involve integrating the operations and internal infrastructure for management operations. The coordination of the activities of these management loops amongst different terminals of the military system is achieved using integrated coordination infrastructure. The majority of modern military systems do not work in separated form or in isolation. Therefore, a powerful demand exists for interoperability with different civil and military systems. Interoperability means that a system should be able to produce the services and should be compatible with other services from other systems [25].

Interoperability includes the capability of moving data from one unit to another amongst several different units in IADS [26]. An interoperable cryptographic task introduces support for various coalitions with scalable architecture. The authentication solutions for the proposed cryptosystem are considered to be pre-shared secret keys of multi-symmetric ciphers with scalable lengths of dynamic one-time ciphering key like those in [27]. The integration of security systems in the majority of IADS is important to protect radar information from unauthorised access [28]. Thus, the adoption of arbitrary cryptographic algorithms from the pool of algorithms and construction of its phases from hundreds of distinct stages provide additional security layers. The main features of the proposed models are provided as follows:

- interconnecting several distributed military databases,
- integrating several command and control systems of different parts into a standard united infrastructure,
- supporting real-time communications and air picture synchronisation,
- coordinating several unmanned platforms and
- providing a secure communication among heterogeneous environments.

## 8. Main Structure of the Proposed Model

The proposed cryptosystem model consists of four main phases, in which each phase may include hundreds of mathematical stages. Each stage is responsible for generating diffusion or confusion properties and the set of different stages constitutes the round transformations. The selected round stages are iterated on the basis of a predefined number of rounds for a new algorithm:

### A. Non-Linear Phase

This first phase contains over 300 stages represented by the S-box and is generated on the basis of 30 different irreducible polynomials in the order of eight as explained in [29] along with several various affine equations. The pseudo code is provided as follows:

```
Cin>>F
Switch (F)
{
Case1: S-Box1
Break;
Case2: S-Box2
Break;
.
.
Case300: S-Box300
Break;
      default:
      cout << "\n Wrong Number.";
break;
}
```

### B. Shifting and Rotation Phase

The second phase in the proposed cryptosystem is responsible for its diffusion properties and contains 100 different rotations and shifting. The pseudo code is provided as follows:

```
Cin>>G
Switch (G)
{
Case1: Shifting1          //Shifting Rows
Break;
Case2: Shifting2          //shifting Columns
Break;
Case3: Shifting3          //Knight move Shifting
Break;
Case4: Shifting4          //Zigzag Shifting
Break;
.
.
Case100: Shifting100      //Reversible Shifting
Break;
      default:
      cout << "\n Wrong Number.";
break;
}
```

### C. Linear Phase with MDS Coding

The linear phase involves over 175 different equations of 4, 5, 6, 7 and 8 degrees with polynomial matrices. The pseudo code is provided as follows:

```
Cin>>H
Switch(H)
{
Case1: MDS1                        // MDS of Order 4
Break;
.
.
Case100: MDS100
Break;
Case101: MDS101              // MDS of Order 5
Break;
.
.
Case125: MDS125               // MDS of Order 6
Break;
Case126: MDS126
Break;
.
.
Case150: MDS150               // MDS of Order 7
Break;
Case151: MDS151
.
.
Case175: MDS175              // MDS of Order 8
Break;
      default:
      cout << "\n Wrong Number.";
break;
}
```

### D. Key Generation Techniques

The proposed cryptosystem includes a set of different advance techniques. These methods are responsible for generating the ciphering keys in different modes and the directory list that stores thousands of strong pre-generated ciphering keys, which are digitally indexed as expressed in the following pseudo code:

```
Cin>>B
Switch (B)
{
Case1: Ciphering Key1
Break;
.
.
Case10000: Ciphering Key 10000
Break;
```

```
        default:
        cout << "\n Wrong Number.";
break;
}
```

Apart from the four main phases, some important settings in the packet must be addressed, such as message length, state array dimension, ciphering key length, ciphering key number and number of rounds as shown in Fig. 4.

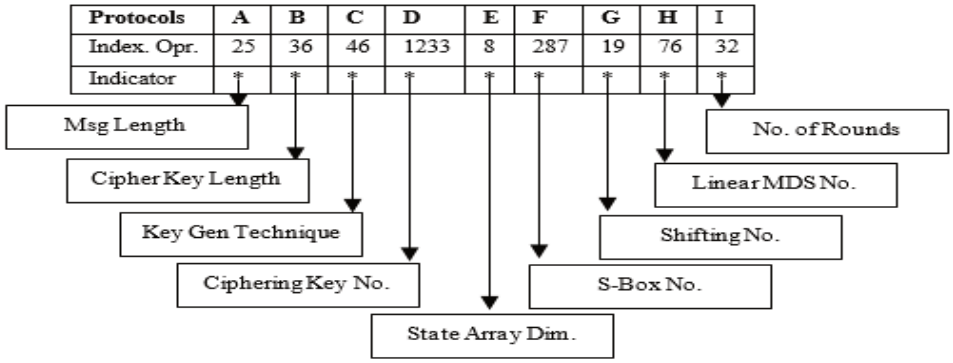


*Fig. 4 Handshaking packet with the indexer of operations*

## 9. System Analysis and Investigation

The proposed system is a multi-target engagement system that works in IADS as an effective unit. The system can simultaneously verify hundreds of targets. The suggested system can also establish multi-authentication sessions with multi-objectives concurrently with an independent changeable algorithm for each session. Each algorithm in the proposed system is designed to be similar to the work of the AES cipher [30] and may be the same size or have an extended form. The search space and guessing possibility are extremely difficult and impossible for hundreds of different dynamic algorithms rather than for one static algorithm. Therefore, brute force and dictionary attacks, apart from the majority of known attacks, are ineffective and inapplicable. The reason is that all the algorithms in the proposed model are continuously changeable and in dynamic form. Therefore, the radar will build a suitable algorithm according to the nature of the situation it determined and the required complexity level.

The enemy cannot analyse the intercepted message through the handshaking procedure because of the limited time and verification requirements, which include no delay in responding. Accordingly, this situation will lead to dangerous engagement. All handshaking operations between the target and radar occur automatically except for the radar-selected operation number, which is chosen manually. The opponent must obtain the complete mathematical operations for the system and the same indexing guide for the operations number to identify the function of SEU. Note that owing to the sizable number of equations, mathematical proofs and S-boxes tables, such aspects cannot be explained thoroughly in this study because of limited scope and the large size of the proposed system. The dynamic nature of the proposed model would prove difficult for the majority of malicious attacks to be effective. The execution time for session establishment differs from one scenario to another based on the handshak-

ing factors. The algorithm size, key length, number of rounds accompanied by the internal mathematical operations and number of engaged targets and their distances are considered effective factors. These factors play a vital role in the strengths of the session setting-up with multi-targets in real-time engagement. The session management amongst the targets are fully computerised operations except for the handshaking protocols selected from the operations centre or the end user. Fig. 5 depicts the public description for the real-time scenario for session management and handshaking engagement process.

The majority of IADSs are developed and operated on state borders to protect countries from external aggressions. Permission given to targets to enter a country's airspace and territorial boundaries requires authorisation by the country itself to preserve security and sovereignty. The verification of the target begins when the targets approach the borders of the country. The verification process will take a few seconds to determine the nature of the target, whether it will be treated as a friend or hostile target. The reason is that the entire scenario for the engagement and handshaking establishment occurs under an extremely tight timeline.

Cryptanalysis of the system does not require guessing or predicting the internal operations to reveal the secret ciphering keys. The reason is that any process that does not provide the attacker any opportunity to guess or break the ciphering keys would require considerable time. Thus, the airspace of the country will be closed and secured against all parties and can be accessed only by formal request or prior coordination. The lack of such a system by the target will prevent it from proving its identity and thus endanger it if it is close to endangering state sovereignty. If the target should attempt to camouflage or fudge to reveal the system secrets or detect the internal processes, then it will not have sufficient time to exploit cryptanalysis. In this case, the target will be forced to retreat or be exposed to fire.

Airspace is opened in front of allies or friendly forces, who are provided with a set of handshaking protocols previously to enable them to deal with this system as friends or authorised targets. After the elapsed session time for authentication task is completed, the handshaking protocols that have been given to the friendly targets will be disabled. Thus, such protocols are not used more than once without the knowledge of the operations centre. In this system, all known attacks will be impossible because the system operates under a very tight timeline. Lastly, if the system has been compromised or detected by the adversaries, then the operations command or operations centre will produce a different electronic manual. This E-manual guide will involve changing the sequence of processes and algorithm indexing within the system package, which, will generate a high probability space that closes the door to any malicious attacks. The existence of such smart security systems has the following several benefits:

- identifying the targets before they reach the borders with hundreds of kilometres distance by verifying their identity,
- maintaining aircraft and engine consumption and avoiding aviation for thousands of miles to track the targets, consequently reducing fuel consumption and maintenance costs,
- linking all institutions in the country with a unified system that provides secure communication under a standard authorised cryptosystem and

- providing a high-level protection system that protects the borders and sovereignty of a state from external dangers and offers complete control over a system even after exporting or selling the system to friendly countries.

The majority of the algorithms of the proposed cryptosystem package have been tested in terms of randomness. The randomness tests did not identify any gradients or biases towards random deviation. Generally, such tests generated acceptable results. The simulation of time implementations was tested by a set of personal computers that may not be compatible to the actual test in a real-time environment. Different factors can play a drastic role in the measurement requirements in relation to the target distance, radio wavelength, number of targets, target distance and handshaking factors.

*Fig. 5 Real-time operations with multi-targets engagement*

## 10. Conclusion

After the Cold War, several progressive countries developed new intelligent IADSs that combine numerous techniques with secret cryptography. The integrated defence concept involves designing a new protected umbrella of guns, radar, missiles and other types of arms. The suggested system incorporates various techniques into a standard system to face future security challenges and to satisfy the need of army land forces, marine and air defence units. In this study, a new package of a cryptosystem model was submitted as an authentication gate in IADSs for multi-targets. The proposed model is considered a trusted gate of secure access control for authorised parties that can be used for securing borders against external aggression. Moreover, the proposed model can distinguish friendly target from the enemy according to handshaking procedures that depend on the encryption techniques. The developed cryptosystem embeds hundreds of mathematical equations that install the SEU part and keeps it hidden. Exporting countries for these modern techniques maintain the encryption technique completely secret. The manufacturing countries also have complete control over the parts of the IADSs through the SEU that remains idle and can be activated remotely at any time. The proposed cryptosystem package is not limited to military applications and it can be employed in civil applications and other state institutions.

## References

[1] SUSEK, W., KNIOLA, M. and STEC, B. Buried Objects Detection Using Noise Radar. In *Proceedings of the 22nd International Microwave and Radar Conference (MIKON).* Poznan: IEEE, 2018, p. 461-463. DOI 10.23919/MIKON.2018.8405256.

[2] ANDERSSON, K. Modelling the Impact of Surface Emissivity on the Military Utility of Attack Aircraft. *Aerospace Science and Technology,* 2017, vol. 65, no. 17, p. 133-140. DOI 10.1016/j.ast.2017.02.017.

[3] BULLOCK, J.A., HADDOW, G.D. and COPPOLA, D.P. *Introduction to Homeland Security Principles of All-Hazards Risk Management*. Butterworth-Heinemann, 2015, 760 p. ISBN 978-0-12-415802-3.

[4] ROBARDS, M.D., SILBER, G., ADAMS, J., ARROYO, J., LORENZINI, D. and SCHWEHR, K. Conservation Science and Policy Applications of the Marine Vessel Automatic Identification System (AIS)-A review. *Bulletin of Marine Science,* 2016, vol. 92, no. 1, p. 75-103. DOI 10.5343/bms.2015.1034.

[5] PELOSI, M. and HONEYCUTT, A.K. Cruise Missile Integrated Air Defense System Penetration: Modeling the S-400 System. *International Journal of Aviation, Areonautics, and Aerospace,* 2017, vol. 4, no. 3. DOI 10.15394/ijaaa.2017.1104.

[6] MARCUS, C., ANDERSSON, K.E. and ÅKERLIND, C. Balancing the Radar and Long Wavelength Infrared Signature Properties in Concept Analysis of Combat Aircraft – A Proof of Concept. *Aerospace Science and Technology,* 2017, vol. 71, p. 733-741. DOI 10.1016/j.ast.2017.10.022.

[7] SMESTAD, T., OHRA, H. and KNAPSKOG, A. ESM-Sensors for Tactical Information in Air Defence Systems. In *Proceedings of the Systems Concepts and Integration Panel (SCI) Symposium.* Quebec: St. Joseph Corporation Company, 2001, 246 p. ISBN 92-837-1052-5.

[8] ZOTOV, V. and GAO, X. Wide Area Search Munition Delivered by the Intermediate Carriers. In *Proceedings of the 10th IEEE Conference on Signal Processing*. Beijing: IEEE, 2010, p. 1964-1968. DOI 10.1109/ICOSP.2010.5656053.

[9] GRIFFITHS, H. Developments in Bistatic and Networked Radar. In *Proceedings of the IEEE International Conference on Radar (CIE).* Chengdu: IEEE, 2011, p. 10-13. DOI 10.1109/CIE-Radar.2011.6159708.

[10] MALIK, A.A., MAHBOOB, A., KHAN, A. and ZUBAIRI, J. Application of Cyber Security in Emerging C4ISR Systems. *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies,* 2012, p. 223-258. DOI 10.4018/978-1-60960-851-4.ch012.

[11] KAWALEC, A., KLEMBOWSKI, W., WITCZAK, A. and MILOSZ, J. Military Surveillance Radars: From Fixed to Nonrotating Antennas. In *Proceedings of the 16th International Radar Symposium (IRS).* Dresden: IEEE, 2015, p. 967-972. DOI 10.1109/IRS.2015.7226390.

[12] FAM, A.T., KADLIMATTI, R. and QAZI, F.A. Multistatic Radar System Based on Accurate Signature Identification Via Micro-positioning. In *Proceedings of the IEEE Radar Conference.* Cincinnati: IEEE, 2014, p. 1414-1417. DOI:10.1109/RADAR.2014.6875821.

[13] AMIN, S., CLARK, T., OFFUTT, R. and SERENKO, K. Design of a Cyber Security Framework for ADS-B Based Surveillance Systems. In *Proceedings of the Systems and Information Engineering Design Symposium (SIEDS). Char*lottesville: IEEE, 2014, p. 304-309. DOI 10.1109/SIEDS.2014.6829910.

[14] ARBATOV, A., DVORKIN, V. and BUBNOVA, N. *Missile Defense: Confrontation and Cooperation*. Moscow: Carnegie Moscow Center, 2013, 385 p. ISBN 978-5-905046-23-0.

[15] EL-BADAWY, E.A., EL-MASRY, W.A., MOKHTAR, M.A. and HAFEZ, A.S. A Secured Chaos Encrypted Mode-S Aircraft Identification Friend or Foe (IFF) System. In *Proceedings of the 4th IEEE Conference on Signal Processing and Communication Systems.* Gold Coast: IEEE, 2010, p. 1-6. DOI 10.1109/ICSPCS.2010.5709756.

[16] ARIFIN, B., ROSS, E. and BRODSKY, Y. Data Security in a Ship Detection and Identification System. In *Proceedings of the 5th IEEE Conference on Recent Advances in Space Technologies (RAST).* Istanbul: IEEE, 2011, p. 634-636. DOI 10.1109/RAST.2011.5966915.

[17] WANG, S. and QIAO, Y. Research on Intelligent Radar Detection Model in Complex CGF Air Combat Environment. In *Proceedings of the10th IEEE Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC).* Hangzhou: IEEE, 2018, vol. 1, p. 373-376. DOI 10.1109/IHMSC.2018.00093.

[18] LESTRIANDOKO, N.H., JUHANA, T. and MUNIR, R. Security System for Surveillance Radar Network Communication Using Chaos Algorithm. In *Proceedings of the 8th IEEE Conference on Telecommunication Systems Services and Applications (TSSA).* Kuta: IEEE, 2014, p. 1-6. DOI 10.1109/TSSA.2014.7065947.

[19] KARAKO, T., WILLIAMS, I. and RUMBAUGH, W. *Missile Defense 2020: Next Steps for Defending the Homeland, Center for Strategic and International Studies*. Rhode Island Avenue: Rowman & Littlefield, 2017. 160 p. ISBN 978-1-4422-7990-2.

[20] DAWOOD, O.A., RAHMA, A.M.S., and HOSSEN, A.M.J.A. The Euphrates Cipher. *International Journal of Computer Science Issues*, 2015, vol. 12**,** no. 2, p. 154-160. ISSN 1694-0784.

[21] DAWOOD, O.A., RAHMA, A.M.S. and HOSSEN, A.M.J.A. The New Block Cipher Design (Tigris Cipher). *International Journal of Computer Network and Information Security,* 2015, vol. 12, p. 10-18. DOI 10.5815/ijcnis.2015.12.02.

[22] DAWOOD, O. A., RAHMA, A.M.S. and HOSSEN, A.M.J.A. New Symmetric Cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) Cipher. *International Journal of Computer Network and Information Security,* 2017, vol. 9, no. 4, p. 29-36. DOI 10.5815/ijcnis.2017.04.04.

[23] SAGHEER, A.M., AL-RAWI, S.S. and DAWOOD, O.A. Proposing of Developed Advance Encryption Standard. In *Proceedings of the 4th IEEE Conference on Developments in eSystems Engineering.* Dubai: IEEE, 2011, p. 197-202. DOI 10.1109/DeSE.2011.74.

[24] DI LALLO, A., FARINA, A., FULCOLI, R., STILE, A., TIMMONERI, L. and VIGILANTE, D.A. Real Time Test Bed for 2D and 3D Multi-radar Tracking and

Data Fusion with Application to Border Control. In *Proceedings of the 1th IEEE Conference on Radar (CIE)*. Shanghai: IEEE, 2006, p. 1-6. DOI 10.1109/ICR.2006.343162.

[25] HOEKSTRA, W.E. *Tactical Data Links and Interoperability, The Glue between Systems* [Research Report]. [on line]. Netherlands: Defense Technical Information Center Compilation Part Notice ADPO10859, 2001, 9 p. Available from: https://pdfs.semanticscholar.org/42d1/596f87c4002b9c3a784bd7b1bab75ae9fcc3.pdf?_ga=2.14963382.1892544529.1561572117-1139765700.1558626705.

[26] FROGGATT, T.R. Radar Interoperability with Modern Multi-Function Radars – A case study, In *Proceedings of the International Conference on Radar Systems (IET).* Edinburgh: IEEE, 2007, p. 1-5. DOI 10.1049/cp:20070626.

[27] OUYANG, Y.C., JANG, C.B. and CHEN, H.T. A Secure Authentication Policy for UMTS and WLAN Interworking. In *Proceedings of the International Conference on Communications.* Glasgow: IEEE, 2007, p. 1552-1557. DOI 10.1109/ICC.2007.260.

[28] SCIENCES, E., WALES, S., ADELAIDE, C. and PERTH, C. Interoperability of Multi-Frequency SAR Data for Forest Information Extraction in Support of National MRV Systems. In *Proceedings of the International Geoscience and Remote Sensing Symposium.* Munich: IEEE, 2012, p. 3166-3169. DOI 10.1109/IGARSS.2012.6350752.

[29] BAYLIS, J., LIDL, R. and NIEDERREITER, H. Introduction to Finite Fields and Their Applications. *The Mathematical Gazette,* 2007, vol. 72, no. 462, p. 320-335. DOI 10.2307/3619969.

[30] DAEMEN, J. and RIJMEN, V. *The Design of Rijndael: AES-the Advanced Encryption Standard*. Berlin: Springer, 2002, 238 p. ISBN 978-3-540-42580-9.