International Journal on Advanced Science Engineering Information Technology

Vol.8 (2018) No. 2
ISSN: 2088-5334

SWOT : Secure Wireless Object Tracking with Key Renewal Mechanism for Indoor Wireless Sensor Network

Rafina Destiarti A.[#,*], Prima Kristalina[#], Amang Sudarsono[#]

[#]*Politeknik Elektronika Negeri Surabaya (PENS)*
Surabaya, Indonesia
[*]*Institut Teknologi Telkom Purwokerto*
Purwokerto, Indonesia
E-mail: rafina@ittelkom-pwt.ac.id,{prima,amang}@pens.ac.id

Abstract*— Tracking system is one of concerning issue in wireless sensor network (WSN) application. The accuracy of the location estimation from nodes is important parameter in tracking system. However, many various attacks try to manipulate the estimated location or try to provide false nodes data transmission. The secure and privacy data sharing of the estimation is also become another priority in WSN. Hence, this paper focuses on employing secure wireless object tracking (SWOT) system which is added by the reliable method in privacy data sharing. By proposing the transmission system based cryptographic mechanism, some parameter data that are required in estimated calculation such as RSSI, coordinates, pathloss exponent (PLE), and estimated distance will be hidden using encryption process. Due to the limited computational device, we propose security scheme without raising computational capability. Layered encryption using AES 128, RSA 2048, MD5 and SHA-1 provide high performance authentication and data encryption services for each nodes. Implementing mobile cooperative tracking scenario refers to previous work, the proposed security scheme is efficient in terms of processing time which could not influenced to the estimated location accuracy. Moreover, the authentication protocol which is adopted from one time password scenario can apply the key renewal mechanism for AES 128 and MD5 algorithm. The experimental results show that SWOT system achieves 75.95 ms processing time using Raspberry Pi devices including trilateration algorithm and security process. Meanwhile, PC server consumes around 82.7 ms for decrypting, calculating and showing the estimated position by modified iterated extended Kalman filter (IEKF) algorithm.

***Keywords* — SWOT System; WSN; privacy data sharing; key renewal; Raspberry Pi.**

I. INTRODUCTION

In recent years, there has been rapid development in wireless sensor network (WSN) application resulting a variety of tracking system especially in indoor environment due to the global positioning system (GPS) module limitation. Tracking system can be used in many applications such as battlefield, environmental surveillance, and smart building for determining the object position. Target tracking is part of localization which can show the location information and object trajectory. The location information is typically usefull for enabling many applications such as network configuration and its coverage, deployement system, routing system, location service and rescue, and smart building [1].

Localization based on WSN is estimating the current location of unknown nodes as the target using cooperative communication and some kind of algorithms in wireless manner such as WiFi and bluetooth. There are two kind of nodes in locating system. The nodes whose position are known are called anchor nodes, while the nodes whose position are unknown are called unknown nodes [2]. These nodes Using location of each anchor node and localization algorithm, the unknown node can be determined its position. Afterwards, all estimated position of unknown node can be used for tracking the route or trajectory of the unknown node.

In recent years, many approaches have been proposed tracking system for moving object detection in indoor environment [3]. Typically, the classic methods to estimate the indoor location are time of arrival (TOA), time difference of arrival (TDOA), angle of arrival (AOA) and received signal strength indicator (RSSI) [1][4]. Among the classic methods for indoor location estimation, RSSI-based is the most popular due to its inexpensive cost and easy implementation. On the other hand, the RSSI data have fluctuative data characteristic that can be affected to the location estimation. The fluctuative data from RSSI are influenced by attenuation of the transmitted signal which can be caused by many factors such as shadowing, multipath fading and the obstacle of indoor environment [5]. RSSI-

based localization method which is only used trilateration methods do not fulfil the accuracy requirements for being used in indoor tracking system[6]. Modified iterated extended Kalman filter (IEKF) which has been proposed in [6], is suitable solution for improving the accuracy level, having small computation complexity and low memory compared to the other Bayesian algorithms [7] .

Location tracking system in WSN uses number of algorithms, some of them are used for tracking object and some are used to maintain the quality of tracking. But the important issue is to preserve privacy data of the location information. Tracking object with un-trusted system leads privacy threats due to the sensitive information [8]. Important points to be considered in the tracking object applications are to secure the location of tracked object. In tracking system, the anchor node will be sent the messages to the unknown node as the object periodically. The communication inter nodes via wireless enable the attackers can track those messages to capture the object based on its location messages [9]. Therefore, it is necessary that the tracking object system should be secured enough. The security requirements for tracking system must include privacy of the location information, authorization for validating the nodes and the integrity to identify any kind of irrelevance from true location [10].

However, the cryptographic techniques of security system need a large amount of processing time and many WSN devices are not currently powerful enough to support robust encryption [11]. Hence, processing time become serious concern for tracking system. Therefore, to reduce the processing time, it is desirable to use highly efficient cryptographic techniques for designing security scheme at tracking system. In order to protect the information about the object location, it is necessary to identify the kind of device for each node which have enough computational capability, data store and resource in running the encryption algorithms [12]. The Raspberry Pi crosses both criteria in that it is cheap, effective computer which can be interfaced with other modules to realize systems with immense functionality. The Raspberry Pi microcomputer is capable of implementing a cost effective security system for various applications in WSN [13].

There are several types of attack which can be excuted in tracking and localization system. The attacks are executed in the information collection process in location estimation phase as well as location verification phase. There are two main types of attack, elementary attack which have their own technical aspects of execution involve range change attack and false beacon location attack. Another type is combinational attack are those who merge different tecnicalities of elementary attacks and create overall malicious affect. The combinational attack can be classified into three types (a) impersonation, (b) sybil attack, and (c) location-reference attack [2][10]. Previous work [14] is implementing secure data transmission scheme for localization using RSA 2048 for encrypting the key exchange of AES 128 and MD5 hash function. This schemes is not strong enough for occupying the proper security to defeat the attacks. AES algorithm have difficulty managing their own keys. Therefore security scheme in [14] is yet to be further improved. Key management is an essential prerequisite for security scheme in WSN application. Among the proposed key management schemes, the key renewal mechanism can be an effective solution to provide privacy data sharing from anchor node to the unknown node more securely due to the key freshness [15].

In this paper, we propose a key renewal mechanism for secure wireless tracking (SWOT) system to improve security level and accuracy from previous work in [14]. We adopt the mobile cooperative tracking system using modified iterated extended Kalman filter (IEKF) in [6] which is achieved better performance in accuracy level. The constribution of this paper is adding key renewal mechanism based on one time password (OTP) scenario to the layered security scheme at [14] and implementing this security scheme to the tracking system from [6] using Raspberry Pi as the device at anchor node, unknown node and gateway node. To apply the key renewal mechanism with authentication algorithm, the anchor node as the transmitter are first encrypted the message using AES then authenticated the ciphertext using MD5 during the key establishmet procedure and then the symmetric key of AES algorithm is updated periodically using SHA1 hash functions. The symmetric key of AES and MD5 algorithm are also protected using RSA algorithm. This paper will analyze the processing time and transmission time from each node which can influence to the tracking system performance. The experimental result show that SWOT system has advantage of low processing time, good performance in accuracy of tracking system and stability; moreover, the key renewal mechanism can improve the security level and reduces the overhead in node authentication.

The rest of this paper is organized as follows: The related work of security system applications was discussed in Section II, We presented the proposed SWOT system, including the experimental result to prove the advantage of SWOT system in Section III. Finally, we draw the conclusion in Section IV.

II. Material And Method

In this section, we describe the adopted algorithms which are used SWOT system. Those are trilateration algorithm and modified IEKF algorithm which is used for determining the object position and showing the object route. And also several adopted cryptographic technique such as asymmetric, symmetric, authentication involve OTP scenario for implementing key renewal mechanism.

A. Related Work

The sensor nodes communicate in wireless media makes the network susceptible to several vulnerable events like eavesdropping, unauthorized Haccess, spoofing, replay, and denial-of-service (DoS) attacks [16]. This problem need to be resolved simultaneously along with secured data transmission by the design and implementation of secured WSN particularly for tracking system. The data transmission must satisfies the confidetiality, integrity and availability property of security mechanism. Many researchers have proposed some encryption technique which helps to ensure privacy for protecting data object location in tracking system. The data information of estimated location at server can be accessed only by person who is authorized [17]

Therefore, the security and reliability of privacy data become critical in positioning system like localization and tracking object. A reputation-based security scheme for sensor node localization is proposed in [4] to improve the security and accuracy of sensor localization in hostile or untrusted environments. However, reputation-based security occur in simulation process which cann't be knew the realistic processing time at a device. The advances in of low-power embedded devices, wearables and wireless networks has facilitated the emergence of novel applications for tracking system. Many wireless network devices can not adopt powerful security schemes due to the data storage capacity and processing time which can influence to the power resource. These security schemes should be relevant to the device capability without having an excessive time. The related work [11] present security system using platform which support the interconnection of heterogeneous and ubiquitous object. Using Midgar IoT platfrom as implemented earlier in [11], is not suitable for indoor positioning system that require some devices can transmit some parameter for estimating the position such as RSSI, AoA, ToA and TDoA.

A secure localization approach using mutual authentication and insider node validation has been applied in [10]. The proposed system provides an algorithm to detect the malicious anchor nodes inside the network using location verification schemes based on real location estimation that uses a very less number of control message. The almost same approach from another research on secure localization mobel based on trust valuation in wireless sensor networks is presented. This research also can identify the malicious node using selection process of property set, including estimated distance, localization performance, position information of anchor node and transmission time [2].

The real implementation using microcontroler unit and WiFi as media transmission has been demonstrated in [12]. A wireless authentication center with mixed encryption from RSA, AES and SHA-1 hash function which is called "MEWAC" is proposed. The maximum capability of MEWAC is only using RSA 1024. According to the results, the MEWAC consumes processing time up to 4.89 seconds for RSA-1024 bit. Therefore, the MEWAC also has possibility of further escalation for getting better performance in processing time and improving the security level. On the other hand, the transmission time is also become a concern problem in security system due to the size of data sharing. Data sharing efficiency and security should be focused. When a large scale data needs to be shared, it would be better to split the original file into multiple slices and it is formed into multiple files because the direct link between devices may be disconnected during the transmission. In order to increase the efficiency and to protect the privacy of multiple files, the source node and all the intermediate nodes needs to perform secure network coding operation before sending and receiving the data as proposed in [18].

A number of approaches have been identified in literature review. Almost all the existing works deal with the simulation scenario without implement in real scenario. They also have number of drawbacks such as high processing time, simulator tools usage and predefined knowledge of the network topology. As peer the need of privacy data in tracking system, we propose SWOT system which is extend our previous work at [14], that was proposed secure data transmission scheme using combination cryptographic from AES 128, MD5 hash function and RSA 2048 for mobile cooperative localization system. However, these scenario is not strong enough for providing privacy in key exchange of AES and MD5 algorithm. Therefore, we adding key renewal scenario based on authentication process which is not consumes long processing time as encryption process. In order to apply the key renewal mechanism for AES and MD5 key exchange process, it is necessary to add one-time password (OTP) scenario. This scenario makes it possible to give lifespan and validation in each authentication code which can only be used once and also has expiration period [17][19-21]. In SWOT system, SHA-1 will be used for applying the key renewal mechanism based on OTP scenario. Trilateration algorithm in [14] is resulting small accuracy, due to this problem we combine the tracking system from [6] to the our propose security scheme for increasing the performance of security level and accuracy estimation. All information about parameter for calculating the position such as anchor node ID, coordinates, RSSI value, PLE parameter will be formed into frame data then its frame will be encrypted and authenticated. After that the encrypted frame will be sent to the unknown node in the form of file. For reducing the losses data in transmission phase, we separate the transmission into three times of files using file transfer protocol (FTP). All data frame in those files should be protected before using security scheme. Furthermore, the multiple files can be sent via Wi-Fi communication at raspberry pi device.

B. Symmetric Cryptographic Scheme

Symmetric cryptography uses the same key both for encrypting and decrypting data. These schemes are relatively easy to implement and need only limited computation power for encrypting. However, this scheme have to agree on common key prior to exchanging data. The suitable solution to resolve its problem is replacing the common key at every time which is periodically updated. This solution can be used for ensure more security against eavesdropping [22].

Advanced Encryption Standard (AES) is one of symmetric cryptography scheme. AES is using block cipher as encryption standard by the National Institute of Standards and Technology [19]. The key length of AES are 128, 192, and 256 bits which is known as AES-128, AES-192 and AES 128. In AES algorithm, an encryptor can encrypt data with any size using the symmetric key that have been exchanged before. Therefore, decryptor can only decrypt the ciphertext after receiving the shared key from encryptor [14]. This scheme is vulnerable against capture attack which can be discovered the shared key at insecure wireless communication.

Message authentication can be combined to the symmetric cryptography for checking the integrity of the message. There are two kind of authentication process, the message is directly authenticated it is called MAC (message authentication code), while the massage is formed into ciphertext and authenticated it is called HMAC (Hash

Message Authentication Code). HMAC is formed by combination of encryption and authentication process.

There are three approaches for authenticated encryption using symmetric key: (1) Encrypt-then-MAC (EtM) the message will be encrypted first then HMAC is resulted based on encrypted output, (2) Encrypt-and-MAC (E&M) MAC is formed on message, then the message and the MAC output are encrypted together, (3) MAC-then-Encrypt (MtE) is the reverse form the first approach, MAC is created first, then the MAC output is encrypted. According to the all approaches, the best performance with highest security level is EtM because the message in secured condition and having integrity for getting the secured message. This approach becomes a standard method to ISO/IEC [23]. Based on this reason we addopt EtM approach for this system and also combining with another algorithm for the key exchange scenario which should be designed in low processing time.

C. Asymmetric Cryptography Scheme

Another solution to the problems of symmetric cryptography scheme in security level is asymmetric cryptography[22]. Asymmetric cryptography schemes is designed for encrypting the information using public key (P_k) based on the concept of oneway threshold functions, such as the integer factorization problem, solving the discrete logarithm problems[24]. RSA encryption algorithm is one example of asymmetric encryption scheme which utilizied are pair of keys. The public part of the key is made available to everyone. The private part will always remain in the owner of the key-pair. RSA ciphertext is formed by two large prime number multiplication which is very easy thing, while to detemine the two prime numbers again is very difficult. RSA algorithm for encrypting and decrypting can be described as follows [24]:

- **Setup**: This phase is show the preparation in determining the security parameter. The main parameter of RSA is public key (P_k) and secret key (S_k). The key are resulted from two prime numbers p and q which have multiplied process as r = p.q. The euler function φ(r) is calculated as φ(r) = (p-1).(q-1). The value of S_k can be determined from P_k . $S_k \equiv 1(\text{mod } \varphi(r))$. However, in this system the key is not manually calculated as its equation. The key is determined by OpenSSL Key Generator which is suitable with the size and the calculation of RSA. It randomly generates the node's S_k and P_k.
- **Encryption**: anchor node will act as the encryptor. Assuming message M will be encrypted by anchor node with the ciphertext C output which is using the public key as the main parameter. The encryption process can be expressed with this following formulas :

$$C \equiv M^{P_k} (\text{mod } r) \quad (1)$$

- **Decryption**: unknown node is received the message from each anchor node. The message should be decrypted using RSA key pair (P_k and S_k). The output of this process is the real message M with this following equation:

$$M \equiv C^{S_k, P_k} (\text{mod } r) \quad (2)$$

This RSA cryptosystem can be used to solve the problem of security in symmetric cryptographic for occupying the privacy at key exchange phase. The RSA cryptosystem can ensure both confidentiality, integrity and authentication although it has poweful processing time and high memory capacities. Thus, in this paper we are going to apply asymmetric cryptography and making it possible for small sensors in WSN.

D. One Time Password Scenario

One time password (OTP) scenario is designed from the requirement of periodic password replacement automatically in order for providing safe and not misused password [19]. The main idea of OTP is changing the password on each authentication and deriving a static mathematical expression by the actual time of day. The actual time should be counted or synchronized among sender and receiver. The synchronized time is not require complex calculation or certification authority but only a counter to maintain the synchronization [20].

Due to the time counter, the generated passwords cann't be reused. This condition make uneasy for the attacker which will be found the password. OTP provides low possibility the system from sniffing attack. The procedure of OTP scenario can be arranged to this following steps [19]:

1) Declarating the value of timestamp when OTP is generated → T_{OTP}
2) Combining the value of timestamp with the message to be encrypted → $T_{OTP} \| M$
3) Encrypting the combined data from timestamp and the message → $E (T_{OTP} \| M) = CM$
4) Adding some initial digits from encryption output which can be used as OTP identifier →$ID_{OTP} \| CM$

E. Proposed Key renewal Mechanism

According to the problem of AES algorithm key shared, we propose key renewal mechanism with authentication and encryption process for protecting the data information in tracking system. To apply key renewal mechanism, we adopt OTP scenario that used SHA1 as the authentication algorithm and RSA 2048 as the encryption algorithm. While the secret massage will be encrypted then authenticated using AES 128 and MD5 hash function. The AES key will be updated periodically using SHA1 hash function. There are three main procedure of this security scheme based our propose key renewal mechanism, as shown at Fig.1. There are two main procedures: the transmitter nodes give authentication procedure during the symmetric key setup and update symmetric key procedure. The symmetric key in this system will be generated randomly using OPENSSL function as long as the key size requirement.

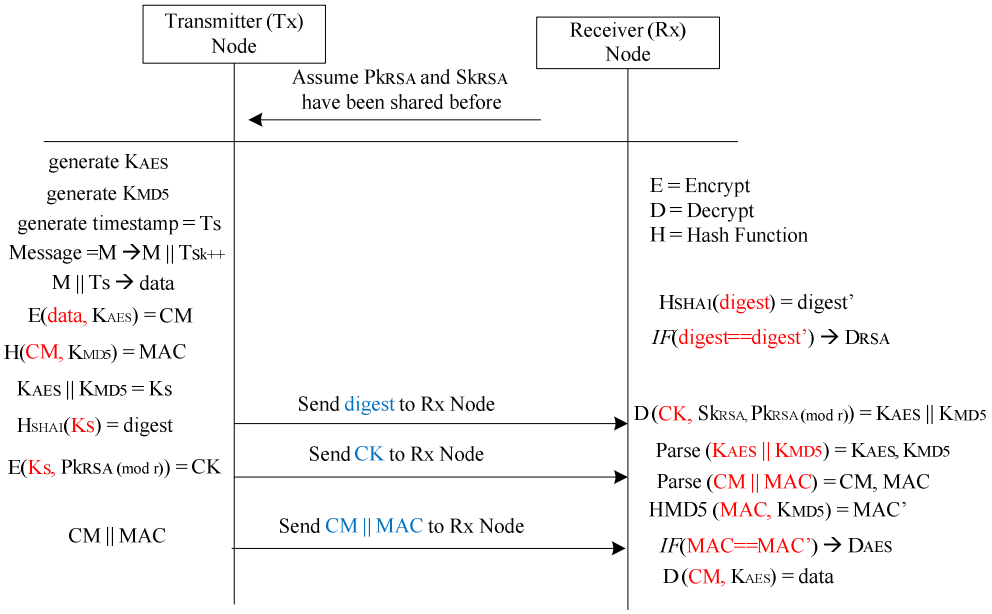

Fig. 1. Proposed key renewal mechanism

Procedure 1: This procedure is related to the preparation process for occupying the parameter in this key renewal mechanism. The first step is the key setup of each cryptography algorithm involve AES 128, MD5 and RSA 2048. The RSA key is assumed that have been shared before, from the transmitter node to the receiver node. Transmitter node is only know the public key (P_k), while the receiver node should be known the pair of public and secret key (P_k , S_k). It is different with AES 128 and MD5. Due to the symmetric scheme and their key should be maintained confidentiality, only the first nodes that can be known the key is transmitter node. Before the key share to the receiver, the key will be encrypted and authenticated. In this section OTP will be applied with timestamp counter (Ts_{k++}). At that moment, the timestamp is combined to the message to be sent being a data frame. Each key from AES and MD5 algorithm is merged into a frame. For having the updated key periodically using authentication process, we authenticate the key frame using SHA1 hash function. Then the digest output from SHA1 can be sent to the receiver node. For increasing the security level of key shared, we can utilized the RSA algorithm which is not required share key due to the public key is open for all devices in this network. The key frame from AES and MD5 will be encrypted using RSA 2048 algorithm. The ciphertext output from RSA can be sent to the receiver node. The multiplication from two large prime number of RSA can make the attacker difficult to access the real message. After transmission process, receiver node can decrypt a message to obtain a temporal key ($K_{0\ AES}$ || $K_{0\ MD5}$). This temporal key should be right for decrypting the real message which have been encrypted then authenticated using AES and MD5. Now, among to the transmitter node and receiver node share a symmetric key, using authentication and encryption phase. It means that the receiver node can guarantee the transmitter node by erasing the temporal key.

Procedure 2: When we try update the key between transmitter and receiver node for the next transmission, transmitter node generate another random key for AES and MD5 algorithm. Thus, the new key will be hashed using SHA1 function and encrypted again using RSA. After that, the transmitter node transmits the digest from SHA1 and ciphertext from RSA to the receiver node. Simillar to the previous procedure the receiver decrypt and verifiy the message. Therefore, receiver node achieve a new symmetric temporary key ($K_{1\ AES}$ || $K_{1\ MD5}$) for decrypting the other message.

F. Proposed SWOT System

In this system we propose a solution key shared of AES and MD5 using encryption and authentication process from SHA1 and RSA which is adopted key renewal mechanism based on OTP scenario. This security mechanism will be implemented to the mobile cooperative tracking system. There are two main process in this security mechanishm. Those are encryption, authentication at transmitter node and decryption, authentication and verification at receiver node. As shown at Fig. 2, the layered security process can be improved the security level at tracking system . This schemes can be implemented to all communication system at this tracking system such as: anchor node(AN) to the unknown node (UN), unknown node(UN) to the gateway node(GN), and gateway node(GN) to the server.

The original message is encrypted using K_{AES} from AES CBC 128 bit and resulted the ciphertext message (CM). Ciphertext is authenticated using K_{HMAC} from MD5 hash function.

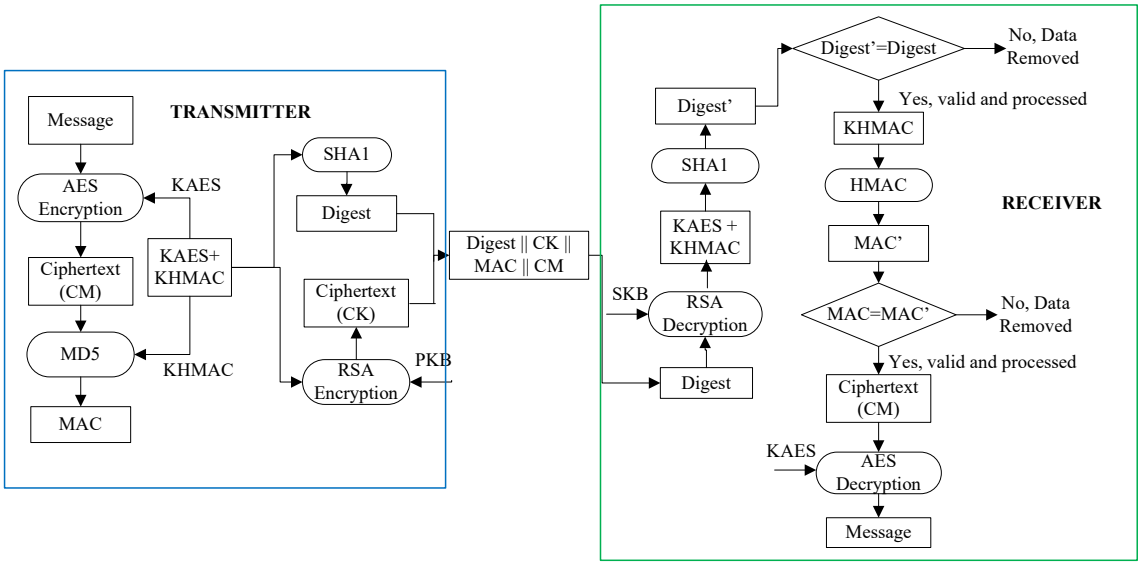

Fig. 2 Proposed security mechanism at SWOT system

Key AES and Key MD5 should be same among sender and receiver. Due to this problem, Key AES and Key MD5 will be combined which is adding some character to separate it. The combining of K_{AES} and K_{MAC} is authenticated using SHA1 hash function. Then, its combination of key also encrypt using RSA 2048. In RSA encryption process, we assume that among sender and receiver are already known the pair key of Secret Key (S_{KB}) and Public Key (P_{KB}).

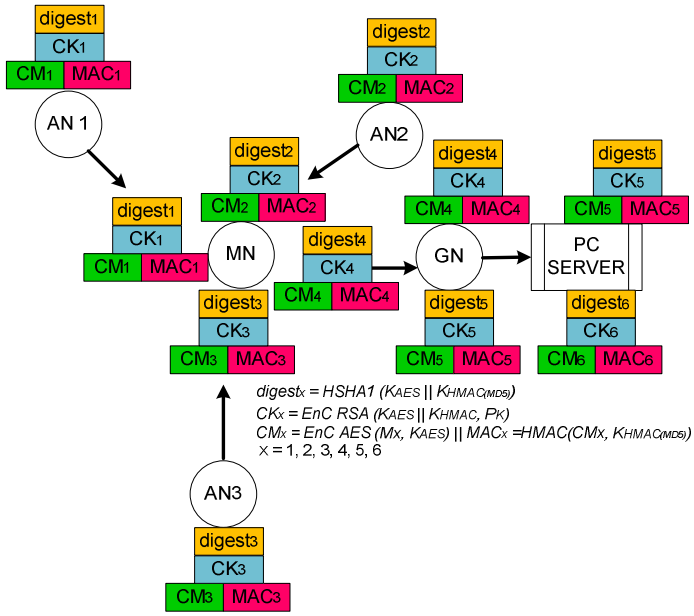

Fig. 2 Data transmission at SWOT system

The output from transmitter part are digest, ciphertext key (CK), MAC and CM. The transmitter will be sent the data into three sessions. At first session, it send the digest due to this digest is using for key verification. When the verification is succesfull, it is proven from the condition of (digest == digest'). Digest' is getting from digest authentication by SHA1 hash function. But if the data is unvalid, this process will be end. But if the data is valid, the receiver node will be received the second data transmission CK. The receiver is decrypt the CK using pair of public and secret key (Pk_B, Sk_B) for getting the AES and MD5 key. Then, receiver node is authenticated the CM using K_{HMAC} based on MD5 hash function. If the MAC from the sender is same with MAC' output of authentication process at receiver, the data is valid and will be processed to the next step which is decrypted the CM using AES CBC 128 bit. But if the MAC is different, the data will be removed. This proposed SWOT system take three times transmission in the formed of files data, as ilustrated in Fig.3. Each AN will be send three files for each transmission including digest at File-1, CK at File-2 and CM||MAC at File-3 to the UN simultaneously. GN is received three files from UN and it will be forwarded to the PC server.

In SWOT data transmission, there are two types of data frame which are formed by parameter data requirement in tracking system calculation, 1) data frame for sending message AN to the UN, 2) data frame from UN to GN or data frame from GN to PC server.

1) Data frame structure from AN to UN

In this system, each AN send some parameters which are required for determining UN position using trilateration. Those parameter are ID of AN, AN coordinate, PLE value, RSSI, deviation standard (Std) and timestamp (Ts). RSSI, PLE, and Std value are used for calculating the distance estimation between AN and UN. Timestamp is additional parameter for applying the key renewal mechanism based on OTP scenario. The Ts value is generated based on the date and the last three digits is based on the route number that have been passed by unknown node.

ID	S	Coordinate X *Anchor*	S	Coordinate Y *Anchor*	S	PLE	S	RSSI	S	RSSI0	S	Std	S	Ts
A1	@	5	@	108	@	1.43	@	-48.2	@	-42.6	@	0.04	@	0611001

Fig. 3. Data frame structure from AN to the UN

Xtri MN	S	Ytri MN	S	D1	S	D2	S	D3	S	X AN1	S	Y AN1	S	X AN2	S	Y AN2	S	X AN3	S	Y AN3	S	Ts
61.68	@	81.62	@	63.3	@	16.1	@	83.2	@	5	@	108	@	70	@	72	@	140	@	108	@	0611001

Fig. 4. Data frame structure from UN to the GN and GN to the PC server

Each parameter is separated using separator in the form of character "@". According to the example data frame structure from Fig. 3, the data length total is 40 bytes will be encrypted using AES CBC 128 bit. The total length of secure frame structure become 144 bytes, combined from ciphertext AES and MAC MD5 hash function.

2) Data frame structure from UN to GN or GN to server

Three anchor nodes (AN) are automatically send the data frame to the UN together using multiple socket based on file transfer protocol. UN also receive directly and process it for getting the original message. From the original message, UN separate the message based on its separator for determining some parameter which will be used for calculating distance and position estimation using trilateration algorithm.

Using RSSI, PLE and Std are resulted the distance estimation as stated to this following equation[5]:

$$d_{n(1,2,3,...n)} = 10^{\frac{RSSI_0 - RSSI_{ij}}{10PLE}} \quad (3)$$

Each distance from AN1, AN2, and AN3 will be used for calculated the position estimation using trilateration algorithm. Trilateration algorithm is also needed another parameter such as *X* anchor coordinate ($X_{n=3}$) and *Y* anchor coordinate ($Y_{n=3}$). The estimation position (x_{tri}, y_{tri}) calculation using trilateration formulas is derived as [6]:

$$x_{tri} = \frac{V_{n-i}(y_n - y_{n-i}) - V_i(y_i - y_{n-i})}{(x_i - x_{n-i})(y_n - y_{n-i}) - (x_n - x_{n-i})(y_i - y_{n-i})} \quad (4)$$

$$y_{tri} = \frac{V_{n-i}(x_n - x_{n-i}) - V_i(x_i - x_{n-i})}{(y_i - y_{n-i})(x_n - x_{n-i}) - (y_n - y_{n-i})(x_i - x_{n-i})}$$

Where

$$V_{i(1,2,3,..n)} = \frac{(x_n^{\,2} - x_{n-i}^{\,2}) + (y_n^{\,2} - y_{n-i}^{\,2}) + (d_n^{\,2} - d_{n-i}^{\,2})}{2} \quad (5)$$

The position estimation will be combined with point route number and the other parameter data which will be used for calculating its route estimation using modified IEKF. Those parameter are estimated position coordinate, estimated distance based on each AN and route number based timestamp code. There are 55 bytes characters at Fig. 4 that will be encrypted using AES CBC 128 and this output will be authenticated using MD5 hash function. The total size of this secure data frame is 176 bytes. It show that the size of secure data frame is always different due to the character number for getting encryption process. The task of GN is only forwarding the data to the server. Therefore GN is also used this frame data structure for sending the message to the server.

The timestamp value will be used for signing the right AN. The sign is used for naming the files which will be process in trilateration method. When, there is not complete name of AN or there is losses data in transmission system, the trilateration method cann't be calculated, as shown in Fig 5. UN will be stayed in the same route for waiting the right message from AN. UN has 15 seconds waiting time and 5 seconds for moving to the next position. While in 15 seconds the right message still not received, UN will be erased the previous data and moving to the next route and receiving the new data from AN.

After the three right messages have been received and the position have been determined, UN will be send message to GN using data frame as depicted at Fig.4. Then, GN forward the message to the server. The modified IEKF is processed at server based on received data from GN. The main idea of modified IEKF is combining the trilateration algorithm with conventional EKF algorithm. There are three process for applying this modified IEKF involve initialization state, update state and predict state as the original EKF algorithm. The initialization variables can be described as follows [6]:

$$x_k = [x_{tri} \quad y_{tri}] \quad (6)$$

The value of z_k is used distance estimation from 3 nearest anchor node that can be described as follows:

$$z_k = [d_{est1} \quad d_{est2} \quad d_{est3}] \quad (7)$$

$d_{est(1,2,3)}$ is the distance estimation of mobile node to the anchor node that was obtained from PLE value eq. (3). The covariance matrix is obtained from the coordinate estimation of trilateration method that is described to this following matrix:

$$P_0 = \begin{bmatrix} \sigma^2 x_{tri} & 0 & 0 \\ 0 & \sigma^2 y_{tri} & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad (8)$$

The variable that has been declared before in eq. (6)(8) will be predicted to the next state using the predict state with this following equation:

$$x_k = [x_{tri} \quad y_{tri}]^T * F \rightarrow F = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (9)$$

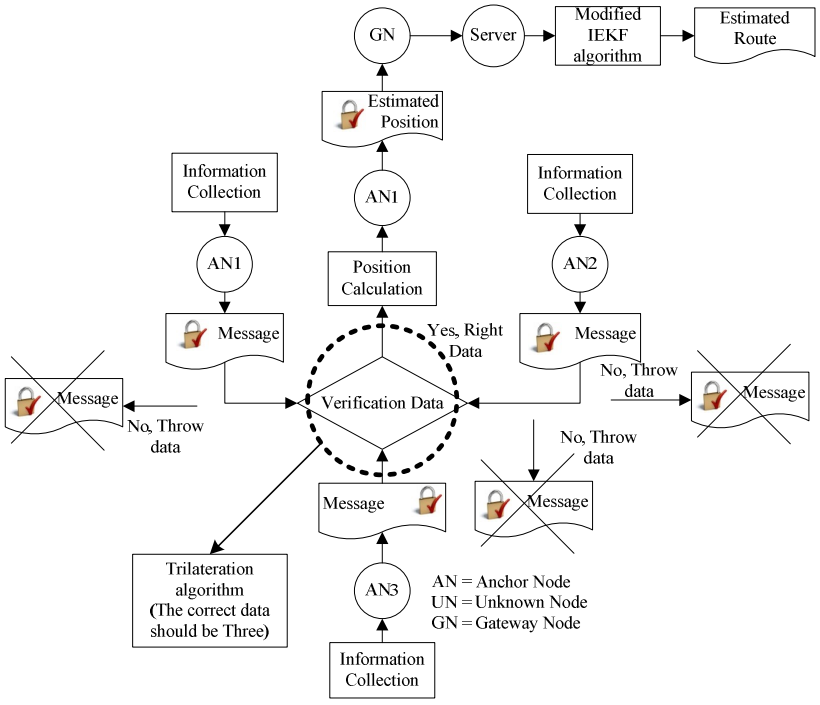

Fig. 5 SWOT system inter-node communication

$$P_k = F * P_0 * F^T + Q \rightarrow Q = P_0 \quad (10)$$

P_k is information state that related with covariance information data before and Q is matrix covariance. The update state from eq.(8-10) will be multiplied with the Kalman gain (K_k). The value of K_k is derived as:

$$K_k = P_k . H_k^T . S_k^{-1} \quad (11)$$

The declaration value of K_k is influenced by jacobian matrix H_k that is expected result of estimation data to the real data, and also influence from updating noise or covariance matrix (P_k, S_k). The update state can be obtained using this following equation:

$$H_k = \begin{bmatrix} \frac{x_{tri1} - x_{anchor1}}{dist_1} & \frac{y_{tri1} - y_{anchor1}}{dist_1} & 0 \\ \frac{x_{tri2} - x_{anchor2}}{dist_2} & \frac{y_{tri2} - y_{anchor2}}{dist_2} & 0 \\ \frac{x_{tri3} - x_{anchor3}}{dist_3} & \frac{y_{tri3} - y_{anchor3}}{dist_3} & 0 \end{bmatrix} \quad (12)$$

$$dist_{k(1,2,3)} = \sqrt{(x_{tri(k)} - x_{anchor(k)})^2 + (y_{tri(k)} - y_{anchor(k)})^2} \quad (13)$$

Covariance matrix value S_k is calculated by combination of covariance matrix P_k from update state which is added with noise variance of distance estimation R_k derived as:

$$S_k = H_k . P_k . H_k^T + R_k \rightarrow R_k = diag(\sigma^2 d_{est1} \quad \sigma^2 d_{est2} \quad \sigma^2 d_{est3}) \quad (14)$$

According the update state, the value of P_0 that has been declared before is derived as:

$$P_0 = (P_k - K_k * H_k) * P_k \quad (15)$$

It also influence to the observation matrix that can be calculated as follows:

$$y_k = z_k - h_k \rightarrow h_k = [dist_1 \quad dist_2 \quad dist_3] \quad (16)$$

The posterior state which is estimation result from EKF algorithm will be resulted coordinate output (x_{EKF}, y_{EKF}):

$$x_k = x_k + K_k . y_k \quad (17)$$

IEKF can be applied based on its number iteration. The first iteration is the output from conventional EKF. The next iteration is using the output of conventional EKF as the initial state for replacing the trilateration output at first iteration process. In this SWOT system, those are four iterations process that can be decreased the error estimation. However, the reduction of the estimation at each iteration is always difference. Modified IEKF is the suitable solution for adding the selection process. This selection process will be started by select the lowest error from each iteration with an average value approach. The example case is when the result in one point route have four estimated data, using the average value approach, the data will be compared with the real data. From this comparation result, the nearest data or the lowest estimated error will be selected as the estimated result from modified IEKF. Using this algorithm, the reduction will be stable although each iterations is not constatly reduce [6]. Combining the modified IEKF algorithm with security mechanishm is expected for providing the tracking system with better accuracy, having the privacy data and achieving the low processing time in WSN device.

III. RESULTS AND DISCUSSION

In this section will be described the real implementation of SWOT system using mobile cooperative tracking scenario. The network model of SWOT system which is consist of network deployment and node devices spesification will be presented in this section. There are two parameters for analyzing the SWOT system performance, those are processing time and transmission time. Due to the accuracy of tracking system have been analyze in the previous

reserach [6], we only focus to the security performance when it combine with tracking system.

A. *Network Model*

Indoor mobile cooperative tracking is a WSN system which contain Anchor Node (AN), Unknown Node (UN), Gateway Node (GN) and Server. There are three AN as the transmitter where it deploy at 0.6 meter height of the wall. One UN as the tracking object receive message from each AN and also send the message to the GN. GN is only receive the message and forward it to the server. Server will be show the estimated result involve position using trilateration and route using modified IEKF. Inter-nodes communicate using FTP via WiFi at Raspberry pi device which is implemented in ad-hoc network. The realistic scenario of SWOT system had been placed at indoor environment of 3rd floor PENS postgraduated building.

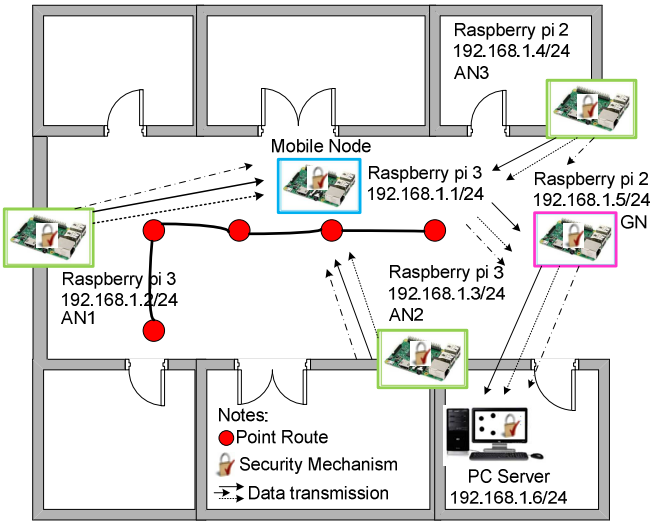

Fig. 6. SWOT system topology

Due to the limitation of device number, we use different type of raspberry pi which can be influenced to the SWOT system performance. The spesification of device and some software addition which can be supported the security mechanism are listed at Table 1. The AN send the message to the UN at every 20 seconds. The UN is waiting the message up to 15 seconds. After the position is determined, the UN is automatically send the message to the GN and forward the message to the server without the waiting time. In server, there are two running systems in different program. Server is always stayed for waiting the sending message from GN. The visualization system for showing the estimated position is using realistic building layout in Java Netbeans Software. The realistic building layout is always running for monitoring the entered data to the resource and than processing it using modified IEKF. The estimated position is automatically shown into the realistic sketch of PENS building. After all estimated position result have been determined, the server calculated the route based on the trilateration algorithm output using modified IEKF up to four iteratons number. According to the Fig. 6, mobile node will pass five point route at every two meters distance which require 5 seconds for each movement.

This SWOT system is using distributed calculation and centralized calculation for tracking object. The distributed calculation will be held on UN. It means that UN has capability in estimated distance calculation based on RSSI value, position estimation using trilateration algorithm, and security process involve encrypt, decrypt and authenticate. While, the centralized calculation will be held on server for processing each estimated position from UN using modified IEKF algorithm. AN, GN, and server also have capability in security process for protecting the message in each transmission.

Table 1. Node devices spesification

Nodes	Devices	Spesifications
AN1, AN2, UN	Raspberry Pi 3	▪ **Networking** 2.4 GHz 802.11n Wireless ▪ **CPU** 4x ARM Cortex-A53, 1.2 GHz
AN3, GN	Raspberry Pi 2	▪ **Networking** TP-link TL-WN725N 2.4 GHz 802.11 b/g/n. ▪ **CPU** quad-core ARM Cortex-A7, 900 MHz
Server	Laptop Toshiba satellite L630	▪ **Networking** Wi-fi 2.4 GHz 802.11 b/g/n. ▪ **CPU** intel core i3-330 M
Software and OS Addition		
gcc-4.4.6, openssl-1.0.1t, Raspbian Noobs, Ubuntu 15.04, Netbeans IDE 8.1		

Due to the large message size output from encryption process and avoiding the losses message, each node of this system is transmitted and received the messages in the form of files at thrice. Each transmission file is corellated with the security scheme requirement. Topology of the proposed network model is shown at Fig.6. All ANs directly send the messages to UN together. UN receive three different messages simultanously each 2 meter movement.

B. *Performance Analysis*

In this section will be discussed the performance analysis of this system. There are three performances which were evaluated in this system. those are processing time, transmission time, and security evaluation from some attackers. Processing time is releated to the encryption, decryption and authentication time from each algorithm. Preparation time invole the needed time for key setup, file generation (reading and writing), and the other required variabel preparation are also calculated in processing time. While, the synchronization time is the performance analysis which is corresponded to the transmission time between transmitter node and receiver node.

1) *Processing Time Analysis*

Regarding to the our proposed security schemes have been successfull implemented in achieving same result message between sent messages and received messages, will be affected to the success of a estimated position and

tracking object calculation. In this section will be analyzed the processing time from the proposed security schemes in conjuction with the tracking system. There are some parts of the processing time analysis, such as preparation time for generating random key, file formation, and frame data structure initialization. Synchronization time, encryption time, decryptiom time and authentication time become analysis parameter in processing time performance. This performance are compared based on the node task and node devices. It is because of different task and capability devices will be influenced to the processing time performance.

According to the data result at Table II., It proves that preparation time at receiver node is larger than transmitter node. There are many processes which have been occured in transmitter node such as separating the received message, creating file, generating key for RSA 2048 bit, and declarating another required variable. The synchronization time is the required time for determining port and IP address destination which can be connected and also received the messages from transmitter node. This condition is also affected to the larger synchronization time of receiver node than transmitter node due to the receiver node should be connected the IP and port to the many transmitter, while the transmitter is only connected to one definite receiver. The largest preparation time is achived by UN as the receiver node from three AN at 3.54 ms and 6.75 ms for the synchronization time.

Table II. Preparation time and synchronization time performance

Transmitter Node	Prep. Time (ms)	Sync. Time (ms)
Anchor 1 (RASPI 3)	1.52	0.24
Anchor 2 (RASPI 3)	1.57	0.27
Anchor 3 (RASPI 2)	2.24	0.52
Unknown (RASPI 3)	1.73	0.22
Gateway (RASPI 2)	1.61	0.45
Receiver Node	**Prep. Time (ms)**	**Sync. Time (ms)**
Unknown (RASPI 3)	3.54	6.75
Gateway (RASPI 2)	4.47	7.02
PC Server	0.91	1.92

Furthermore, the processing time of security algorithm is resulted that encryption process is required faster time than decryption process, as listed at Table III.. In decryption process, it happens for returning the ciphertext message to the original message which is required more complexity calculation than encryption process. From the kind of algorithms result show the RSA algorithm obtain larger processing time than AES, MD5, and SHA1 algorithm up to 3.02 ms in encryption process and 84.16 ms in decryption process. While for the authentication process is required long time at the receiver node due to the verification process after having the authentication process. The function of verification is for checking the similarity MAC and digest, it is same or not compared to the received message and the output of authentication process at receiver. Both of MD5 and SHA1 hash function consumes longer processing time up to 0.128 ms.

Then, the processing time of estimated position calculation at UN is relative fast using trilateration algorithm which is only required 0.037 ms at raspberry pi 3 of UN. This algorithm is capable for implementing to another device of WSN application. It is different to the tracking object calculation for determining the route estimation from the UN as the object. Using modified IEKF at the PC server still require long processing time due to the iterations number and modification algorithm. The experimental result represents that for estimating the passed route of UN from five points movement consumes 65.25 ms processing time. The RSSI, PLE number, and standard deviation data have been measured before in offline phase. In this system, we test the tracking system algorithm using offline data for knowing the influence of security system based on its processing time and transmission time will make losses data or not. As long as the accuracy level requirement, applying the modified IEKF to SWOT system still achieves small error estimation at 1.11 meters for five points movement as shown at previous research [6] without the security system.

Table III. Security algorithm processing time

Transmitter Node	AES Encrypt (ms)	MD5 Auth. (ms)	SHA1 Auth. (ms)	RSA Encrypt (ms)
AN1 (RASPI 3)	0.058	0,034	0.037	2.19
AN2 (RASPI 3)	0.067	0.032	0.038	2.07
AN3 (RASPI 2)	0.093	0.086	0.096	3.02
UN (RASPI 3)	0.069	0.034	0.041	1.71
GN (RASPI 2)	0.099	0.097	0.102	2.21
Receiver Node	**AES Decrypt (ms)**	**MD5 Auth. (ms)**	**SHA1 Auth. (ms)**	**RSA Decrypt (ms)**
UN (RASPI 3)	0.108	0.088	0.097	61.33
GN (RASPI 2)	0.121	0.123	0.128	84.16
PC Server	0.016	0.013	0.021	7.82

The devices type at SWOT system is also influenced to the processing time result. It is related to the processor types at the devices. The processing time which is resulting from node with Rapberry pi 3 is more quickly than Raspberry pi 3 due to the updated version of Rapberry pi 3. Likewise to the PC server can be processed the RSA encryption and RSA decryption only need 2.21 ms and 7.82 ms.

2) Transmission Time Analysis

Transmission time is greatly affect to the security system especially in the wireless media transmission. There are three factors that can be influenced to the transmission time performance. Those are the transmission distance, the size of transmitted file and the link communication device between transmitter and receiver. At SWOT system, there are three times files transmission process. In the first file is containing the digest from SHA1 in the size of 41 bytes. While the second file is containing chipertext result from RSA encryption at 256 bytes. The file size at the last transmission is about 176 bytes based on the combination output from AES 128 ciphertext and MAC of MD5 hash function.

In transmission time measurement, all time setting should be same and synchronized due to the small difference will be influenced to the result. Before having measurement process, all node and PC server should be used NTP server for synchronizing the time. As resulted at Fig. 7., the inter-node distance can be affected to the transmission time result. The measurement of transmission time is occured between transmitter and receiver from 1 meter up to 30 meters distance separation. The retrieval data of transmission time are taken three times for each diplacement, than it will be calculated its average value for each file size. From this experiment, we can know the relation between the size of file and the transmission distance. The result show that for sending each file (File-1, File-2, and File-3) is required larger time when the separation distance is getting further. File-2 with largest file size consumes 45.03 ms at 30 meters distance, while the smallest file size from File-1 only consumes 33. 05 ms at 30 meters distance.

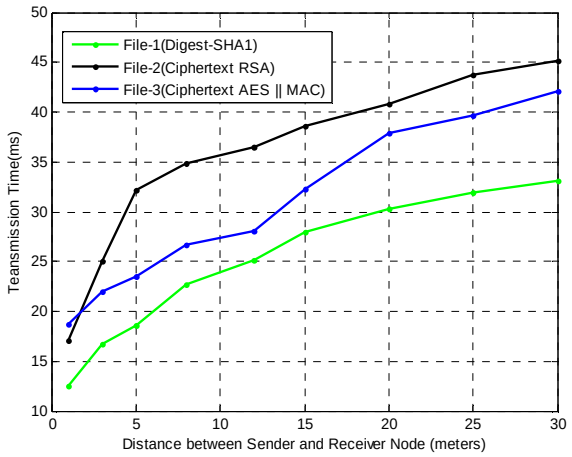

Fig. 7. Transmission time based on various message sizes and distance

The environment condition is also influenced to the transmission time result. Those conditions are line of sight (LOS) and non line of sight (NLOS). LOS and NLOS condition are measured from from GN to PC server transmission. In NLOS condition, server is placed at room, and server is placed at hallway of building to the GN position with 15 meters maximum distance. NLOS condition have sigificant effect to the transmission time up to 59.65 ms for sending File-2 at 15 meters distance. NLOS condition can make the signal transmission being obstructed by the wall or any obstacles in indoor environment. The increasing of transmission time can be affected to the failure decryption process due to the corrupt or losses received data in transmission process.

Another factor for increasing the transmission time is the devices types of this system. It is resulted at Table IV., transmission time for sending file-2 message between AN2 to the UN at 5 meters distance that used same device from WiFi at Raspberry Pi 3 is only required 3.77 ms. It is different with transmission time between AN3 to the UN that reach transmission time up to 14.85 ms. The increasing of transmission time is also founded at GN to the server up to 44.67 ms. This problem is caused by the different types of WiFi devices require additional time for syncronization for making communication channel among them.

Table IV. Transmission time result based on link communication types

Link Communication Types	TT1 (ms)	TT2 (ms)	TT3 (ms)
AN 1 to MN (Raspi 3 to Raspi 3)	4.98	5.97	5.44
AN 2 to MN (Raspi 3 to Raspi 3)	2.66	3.77	2.9
AN 3 to MN (Raspi 2 to Raspi 3)	8.74	14.85	10.64
MN to GN (Raspi 3 to Raspi 2)	7.14	9.02	8.24
GN to *server* (Raspi 2 to PC)	39.85	44.67	42.55

3) Security Schemes Evaluation

In this section will be discussed the security strength using attacker node as the fake node. This fake node will be connected to this network system. The number of fake nodes are followed to the node types of this system. Attacker can act as the AN, UN, GN and server. The fake node pretend as the transmitter for sending the malicious message that can delay the transmission time and simplify the attacker for getting the original message. When the fake message is received by valid node, the valid node cann't verify the message using SHA1, so the system will be automatically exit. While at the File-1, the valid node is successfull for authenticating and verifying the fake message, the valid node is received the second message but it cann't be decrypted due to the key pair (P_K, S_K) of RSA are different. But if the valid node can decrypt the message of File-2 which is using RSA algorithm, the next decryption process in AES algorithm will be failed due to the key between sender and receiver must be same. Invalid data from the fake node will be resulted invalid MAC at data integrity checking. The attacker will be unsuccessfull for getting the real data because there are some corellation data using key renewal scenario between sender and receiver. On the other hand, if the attacker have been obtained the key of AES and MD5 at that time, attacker will be failed for obtaining the original message due to the updating scenario at key generation of AES and MD5 algorithm.

Our implementation of SWOT system in indoor WSN satisfies confidentiality including privacy and data integrity of security system properties and also collusion resistance between unknown node to the three nearest anchor node. We analyze the security properties of our scheme as follows:

Data Confidentiality. The information of data location is encrypted using layered security that is formed by layered security schemes from combination of SHA1, RSA, AES, and MD5 algorithm. The data information is encrypted with random symmetric key for AES and then the key shared of AES is protected by RSA, SHA1, and MD5 algorithm. During the decryption phase, only the receiver with valid key that can decrypt the ciphertext. Since the set of 2048 bit pair of RSA key can not recover at the fast time, attacker cann't determine the desired value of key. As well as AES key, when the attacker want to obtain the original message, the attacker should be know the all parameter of security

schemes involve AES and MD5 key which are formed by renewal scenario.

Collusion Resistance. Three anchor nodes may intend for sending the data to the one unknown node which they can send in the same time simultaneously. In our scheme, encryption phase the data without ID of anchor node and timestamp still can be processed when the decryption is succed. During the position calculation, timestamp is important due to the initial name for processing the file at trilateration algorithm. Therefore when the nodes don't have the timestamp, the position the veryfication process and calculation will be failed. It make the UN wait the new message that used renewal key for having decryption and encryption process. Thus, the proposed security scheme is collusion-resistant which is uniquely related to each anchor and makes the ID and timestamp for calculating the position.

IV. CONCLUSIONS

In this paper, we propose SWOT system based on key renewal mechanisms for indoor WSN. There are two main concern at this system, providing the strength level of security with low processing time for small sensor node of WSN and allowing high accuracy for tracking system. Combining asymmetric, symmetric and hash function is one solution for securing the key shared between transmitter and receiver. Adding key renewal mechanisms based on OTP is providing temporary key generation at sharing session. The real message is encrypted using AES and authenticated using MD5 hash function. AES key and MD5 key are protected and updated automatically for each transmission by RSA and SHA1 algorithm. The unknown node as the object is received three message from anchor nodes for calculating position by trilateration algorithm. The estimated result is processed again to the server by modified IEKF algorithm. All link communication process is equipped with our proposed security mechanishm. The performance of processing time result show that using raspberry pi as the transmitter and receiver nodes achieved 96.02 ms maximum time. The size of data, distance between transmitter and receiver, and devices type are influenced to the transmission time. In our future work, mobile tracking system with the ECC algorithm which have smaller processing time and higher level security schemes will be proposed.

REFERENCES

[1] Long Cheng, et. all, "A Survey Localization in Wireless Sensor Network", Hindawi Publishing Corporation International Journal of Distibuted Sensor Netwok, vol. 2012, 12 pages, 16 November 2012.

[2] Peng Li, et. all, "Research on Secure Localization Model Bsed on Trust Valuation in Wireless Sensor Networks", Hindawi Publishing Coorporation, Security and Communication Networks, vol. 2017, 12 pages, 8 March 2017.

[3] Alessandro G., and Stefano Q., "Moving Object Detection in Heterogeneous Conditions in Embedded Systems", Sensors 2017, vol.17, Issue 7, 1 July 2017

[4] Jingsha He, et. All, " Reputation-Based Secure Sensor Localization in Wireless Sensor Networks", Hindawi Publishing Corporation, The Scientific World Journal, Vol. 2014, 10 pages, 20 May 2014.

[5] Rafina D., Prima K., Amang S. "Cluster-Based PLE Areas for Mobile Cooperative Localization in Indoor Wireless Sensor Network", International Conference on Information Technology and Electrical Engineering (ICITEE), pp: 112-117, October 2016, IEEE.

[6] Rafina D., Prima K., Amang S., "Modified Iterated Extended Kalman Filter for Mobile Cooperative Tracking System", International Journal on Advanced Science Engineering Information Technology, vol.7, no. 3, pp. 980-992, 2017.

[7] Rafiullah Khan, Sarmad Ullah Khan Shahid Khan, and M. Usman Ali Khan, "Localization Performance Evaluation of Extended Kalman Filter in Wireless Sensors Network", ANT international conference Procedia computer science, pp:117-124, 2014.

[8] Shrikant P. D., Archana R. R., "Analysis of Location Monitoring Techniques with Privacy Preservation in WSN", 4th International Conference on Communication Systems and Network Technology, pp: 649-653, 29 May 2014, IEEE.

[9] Abhishek Das, Laxmipriya M., "Bypassing Using Directional Tranceivers: A Design for Anti-Tracking Source Location Privacy Protection in WSNs", International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pp: 39-44, 16 January 2016, IEEE

[10] Gulshan K., Mritunjay K.R., Hye-Jin Kim, and Rahul S., "A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks", Hindawi Publishing Coorporation, Mobile Information Systems, vol.2017, 12 pages, 26 February 2017.

[11] Gonzalo S., Cristian G. G., and B. Cristina P. G., "Midgar: Study of Communications Security Among Smart Objects using Platform of Heteregeneous Devices for the Internet of Things", Future Generation Computer Systems, vol. 74, issue 2017, pp: 444-466, Elsevier.

[12] Yiqin Lu, Jing Zhai, R. Zhu, and Jiancheng Qin, "Study of Wireless Authentication Center With Mied Encryption in WSN", Hindawi Publishing Corporation, Journal of Sensors, vol. 2016, 7 pages, 29 May 2016.

[13] Singoee S. S., "Raspberry Pi Based Security System", University of Nairobi, Department of Electrical and Information Engineering, 17 May 2016.

[14] Rafina D., Prima K., Amang S. "Secure Data Transmission Scheme for Indoor Cooperative Localization System", International Electronics Symposium (IES), September 2017, IEEE.

[15] Saewoom Lee, and Kiseon Kim, "Key renewal mechanism with Sensor Authentication under Clustered Wireless Sensor Networks", Electronics letters, vol. 51, No. 4, pp: 368-369, 19 February 2015, IEEE

[16] R. J. Kavitha, B. Elizabeth C., " Secured and Realiable Data Transmission on Multi-hop Wireless Sensor Network", Springer science+Business Media, LLC 2017, 25 September 2017

[17] M. Thangavel, P. Varalakshmi, S.Sridar, " An Analysis of Privacy Preservation Schemes in Cloud Computing", International Conference on Engineering and Technology (ICETECH), pp: 146-151, March 2016, IEEE

[18] Lei Wang and Qing Wang, "Secure-Network-Coding-Bsed File Sharing Via Device-to-Device Communication", Hindawi Publishing Coorporation, Journal of Electrical and Computer Engineering, vol. 2017, 7 pages, 8 June 2017.

[19] Eddy P. N., Rizky R. J. P., and Iman M. R., "SMS Authentication Code Generated by Advanced Encryption Standard (AES) 256 bits Modification Algorithm and One Time Password (OTP) to Activate New Applicant Account", ICSITECH, 2016, IEEE.

[20] Salem Aljareh, and Anastasios Kavoukis, "Efficient Time Synchronized One-Time Password Scheme To Provide Secure Wake-Up Authentication on Wireless Sensor Netwoks", International Journal of Advanced Smart Sensor Network Sytems (IJASSN), vol.3, No.1, January 2013.

[21] Mostafa Abedi, M. Hassan Y., Farshad P., " Fast Location Prediction Algorithm Utilized in Enchancing One Time Password Authentication", IEEE Student Conference on Research and Development, 2012.

[22] Zhang Yu, "The Scheme of Public Key Infrastucture for Improving Wireless Sensor Network Security", International Conference on Computer Science and Automation, pp: 527-530, 2012, IEEE.

[23] Amang S., Toru N., "A Secure Data Exchange System in Wireless Delay Tolerant Network Using Attribute-Based Encryption", Journal of Information Processing, vol.25, pp:234-243, February 2017.

[24] Gaochang Z., Xiaolin Y., Bin Z., Wei W., "RSA-Based Digital Image Encryption Algorithm In Wireless Sensor Network", ICSPS, pp: 640-643, 2010, IEEE.