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.

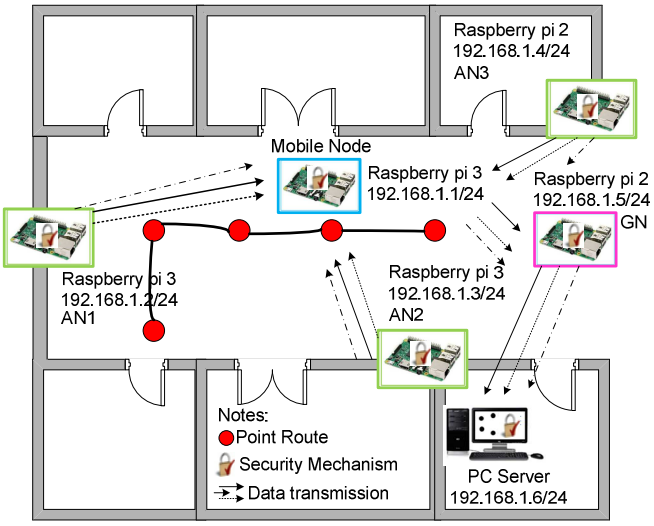

Fig. 6. SWOT system topology

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.

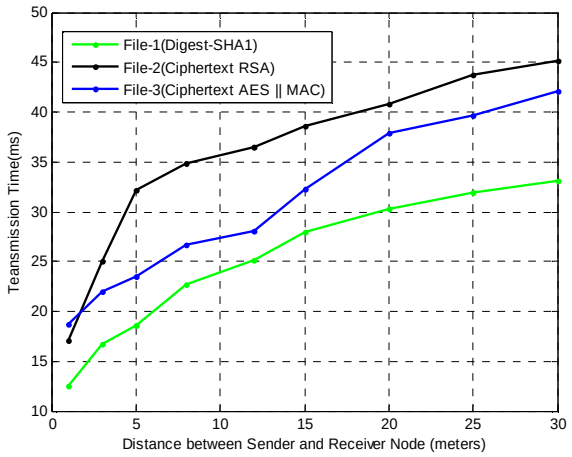

Fig. 7. Transmission time based on various message sizes and distance

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.