International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 4, Jul – Aug 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A Trust-Oriented Key Management Protocol for Cluster-Based Wireless Networks

Dr. R. Jayaprakash *, Dr. A. Kalaivani **
*Department of Computer Technology, NGM College, Pollachi, India
Email: jpinfosoft@gmail.com , jayaprakash@ngmc.org
** Department of Computer Technology, NGM College, Pollachi, India
Email: kalaivani@ngmc.org

Abstract:
One of the protected communication techniques in cluster based privacy preserving MANET is providing a Trusted Key Management Protocol (TKMP). A TKMP calculates a trust key exchanging for all the cluster nodes in the communication for security. TKMP allocates a dynamic private and public key exchanging value for trust variable where it will be checked during communications. The total proposed protocol is executed in three stages, for example, Initial-sending, key creation and validation of key and affirmation. In the primary stage, the cluster nodes are offered with the unique identity (ID), and after that, the following stage utilizes the Paillier cryptosystem (PC) homomorphic encryption model, for making the basic key to the message correspondence. Finally, a geometrical model is created in this work with various variables, for example, a hashing capacity, holomorphic encryption, profile succession, irregular number capacities. The proposed TKMP strategy sets up the verified correspondence over the WSN by the authentication process.

Keywords— Cluster Network, Secure Communication, Key Generation, Key Validation, Homomorphic Encryption

I. Introduction
Cluster-based security models in MANETs remain vulnerable to several security breaches originating from malicious external nodes as well as compromised nodes [3,4]. To protect routing information, packets can be encrypted using an appropriate key-based technique [5-7]. The secure cluster-based routing protocol can be integrated with reactive routing protocols to protect the route-discovery process from attacks that may disrupt it. This allows the identification of routes basedhotspot for evacuation the deceptive reacts and such secure directing conventions will depend totally on the security relationship among the starting point and the objective hub. The security relationship can also be established by using a combined key derived from the public keys of the source node (O) and destination node (T). Nodes O and T use a secret symmetric key (KeyO,T) established with the public keys of one another.

In this work, we develop a secure routing key-management scheme based on the Trusted Key Management Protocol (TKMP), which authenticates public and private keys and applies encryption and decryption mechanisms to protect packets and messages from attackers. The next section reviews recent studies on public-key development methods and introduces the related concepts. Section III presents the proposed TKMP model, including the new trust-key model and its verification procedures. The final section presents the concluding remarks.

II. Background Study
(Azarderakhsh, Reza, ArashReyhani-Masoleh, and Zine-EddineAbid, 2008)[8] stated that the key management in cluster-based wireless sensor networks using both private and public key cryptography. Their objective is to introduce a platform in which public key cryptography is used to create a secure path among sensor nodes and gateways. Instead of pre-loading a huge amount of keys into the sensor nodes, every node desires a session key from the gateway to set up a secure path with its neighbors after clustering phase. The

security examination and performance evaluation showed that the key management method has considerable saving in storage space, broadcast overhead, and perfect resilience against node capture.

(Udaya, D., SuriyaRajkumar, and RajamaniVayanaperumal, 2013) [9]examined a security is one of a significant factor to be viewed as truly in remote sensor systems. In WSN, from multiple points of view interruption may happen, in the history decades there is no ideal IDS, with no squandering of assets like time, vitality, cost and number of physical things. The principle target is to guarantee the security and improve the nature of system by applying a Leader based interruption identification framework in the Wireless Sensor Network (WSN). Here, we are concentrating on the assault known as sinkhole assault which is considered as the greatest risk in remote sensor organize which crown jewels the total correspondence and an information misfortune between a couple of hubs as source hub and a goal hub. So as to give a total answer for identify and dodge sinkhole assault a Leader Based Intrusion Detection System (LBIDS) is proposed. Their methodology a pioneer is chosen for each gathering hubs inside the system, area savvy and it do looks at and figures the conduct of every hub, intelligently executes our identification module and screens every hub conduct inside the bunch for any sinkhole assault to happen.

(Xun Yi, Russell Paulet, Elisa Bertino, 2014) [10] considered the issue that includes executing an encoded focused on commercial framework that creates ads relying upon the substance of a client's email. Since the email is put away in an encoded structure with the client's open key, the email server plays out a homomorphic assessment and processes a scrambled notice to be sent back to the client. The client unscrambles it, plays out an activity relying upon what she sees. On the off chance that the commercial is significant, she may tap on it; else, she just disposes of it. Be that as it may, if the email server knows to this data, to be specific whether the client tapped on the ad or not, it can utilize this as a confined unscrambling prophet to break the security of the client's encryption plan and conceivably considerably recoup her mystery key. Such assaults are omnipresent at whatever point we figure on encoded information, nearly to the point that CCA security appears to be inescapable. However, it is anything but difficult to see that picked ciphertext (CCA2-secure) homomorphic encryption plans can't exist. In this way, a suitable security definition and developments that accomplish the definition is sought after.

(Q. Jiang, S, Zeadally,J. Ma and D. He,2017) [11introduced a lightweight and secure client verification convention dependent on the Rabin cryptosystem, which has the highlights of computational asymmetry. They led a perceived affirmation of the convention utilizing ProVerif so as to display that the strategy finishes the vital security properties. The creators introduced a total heuristic security examination to demonstrate that the convention is secure next to all the potential assaults and gives the ideal security highlights.

(Razaque, Abdul, and Syed S. Rizvi, 2017) [12]expressed that the past secure information collection approaches for remote sensor systems were not proposed for consent, vitality productivity and proper security, leaving them inclined to assaults. The creators presented the protected information accumulation utilizing the entrance control and validation (SDAACA) convention. Utilizing SDAACA convention to see sinkhole and Sybil assaults that are hard to distinguish by existing cryptographic methodologies. The SDAACA convention comprises of two novel calculations: the protected information fracture (SDF) and the hub blend approval (NJA). The SDF calculation secretes the information from the foe by dividing it into little pieces. In the NJA calculation, an approval procedure is started previously enabling any new hub to join the system. The two calculations help improve the Quality of Service (QoS) parameters

(Jaewoo Choi, Jihyun Bang, LeeHyung Kim, MirimAhn, and Taekyoung Kwon, 2017) [13]proposed an area based key administration plot for WSNs, with uncommon thought of insider dangers. In the wake of surveying past area based key administration strategies and examining their benefits and negative marks, they chose area ward key administration (LDK) as an appropriate

technique for their investigation. To unravel a correspondence impedance issue in LDK and comparable strategies, they have concocted another key update process that consolidates matrix based area data. They likewise proposed a key foundation procedure utilizing network data. Besides, they developed key update and denial procedures to adequately oppose inside aggressors. For examination, led a thorough reenactment and affirmed that their method can intensify network while diminishing the trade off proportion when the base number of normal keys required for key foundation is high.

(Ahlawat, Priyanka, and Mayank Dave, 2018) [14]Talked about to diminish the hub catch crash by consolidating a productive antagonistic model for cell model of WSN. The antagonistic model builds up various vulnerabilities introduced in the system, for example, raised hub thickness, task of the sink hub, neighbor weight factor to ascertain the arrangement likelihood of every cell. It at that point depicts the hash chain length for each cell with different rekey period to intensify the system obstruction against hub catch assault. Their technique is contrasted and different past strategies regarding the probability of key trade off and the measure of ways rekeyed. The results affirm its viability in expanding the WSN security.

III. TRUSTED KEY MANAGEMENT PROTOCOL (TKMP)

The primary objective of the proposed TKMP is to design and develop a dynamic key-management protocol based on normal and multi-level authentication within clusters. The proposed protocol consists of three entities—Cluster Head (CH), Cluster Member (CM), and Base Station (BS)—for managing keys within the network. The overall TKMP framework comprises three stages: initial deployment, key creation, and key validation and confirmation. In the first stage, cluster-member nodes receive unique identities. During key creation, lightweight key generation based on enhanced homomorphic encryption is used to generate the required keys. Finally, key validation and verification are performed using a geometrical model incorporating a hashing function, enhanced homomorphic encryption, and random number functions. Thus, the geometrical model developed for key management enables the proposed TKMP to validate the entities and provide secure, dynamic key management in the clustered network. The figure 1 portrays the TKMP procedure stream.

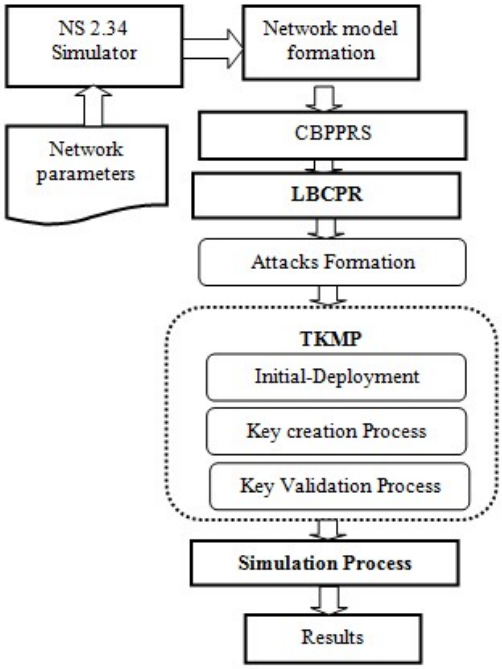


Fig.1: TKMP process Flow

IV. Network Architecture

The network model consists of M nodes randomly deployed within the simulation area. All nodes (N(k)) are dynamic with respect to their creation, location, and availability. In addition to the ordinary nodes, the cluster network contains two specially configured entities: the Base Station (Bst) and the Cluster Head (CH). The CH monitors the behavior of the mobile nodes, records the observations, and forwards the information to the Bst. The network formation is evaluated in graph model was already we presented (R. Jayaprakash, B. Radha, 2018). In the proposed network, each Cluster Member (CM) is assigned a unique ID for validation and authorization. Any node N(k) can broadcast packets to another node N(l) in the network without restrictions R(k). All nodes are capable of dynamically changing their locations. To ensure secure communication, each node is verified through

its ID before it is authenticated and authorized to communicate with other nodes.

V. CBPPRS and LBCPR

Cluster Based Privacy Preserving Routing Selection (CBPPRS) was previously presented (R. Jayaprakash, B. Radha, 2018) thinks about the gathering of Cluster heads (CH) in a portable ado system of n intersections/hubs to such an extent that all hubs in this system are inside separation h jumps of a CH, for a known DEFINED – VALUE.

The Load Balancing Cluster Based Privacy Routing (LBCPR) was previously presented (R. Jayaprakash, B. Radha, 2018) load awkwardness in the system and the inclination or bias in getting halfway found hubs for information move. The proposed a novel group based directing measurement, load and a minimization rule to settle on a choice a way that involves versatile hubs with less burden weight on them In LBCPR performs new measurement called burden will reveals to us the evaluated burden a portable hub (mn) is engaged to in a system, its worth will indicate the evaluate of current burden. In this model, connect looking and send react calculations performs bunch burden field precisely.

Attacker Model

In the model for attacker, The following are done

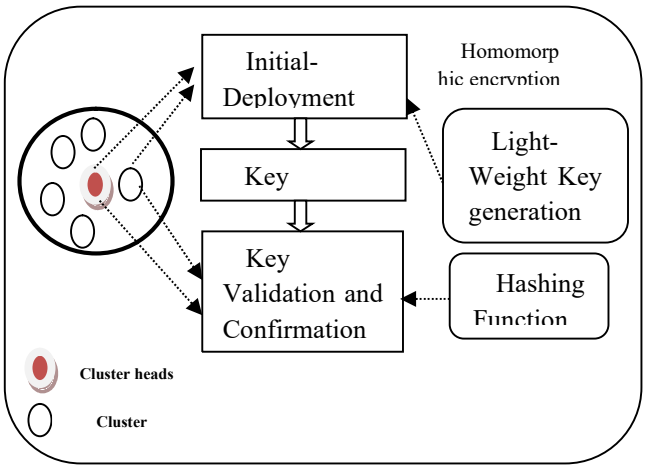
The Attacker is able to capture all of the traffic in the area of network concerned.

The snooping is so promising in the network and the communications and of the knowledge on the nodes that are near by following the message size , etc

Depending on the variation, there seems to be certain possibilities in the attack that drops the packets into the network.

VI. TRUSTED KEY MANAGEMENT PROTOCOL (TKMP)

This part depicts the proposed TKMP, for making a verified correspondence interface in clustered Network. The proposed TKMP performs key management through three distinct stages. The TKMP development process is illustrated in Figure 2. As exhibited in the above figure, the TKMP three stages are 1) Intial-Deployment, 2) Key Creation, and 3) Key Validation and Confirmation. The proposed TKMP can be viewed as an extension of the Paillier cryptosystem (PC), using the public key to support secure communication. The means engaged with the proposed TKMP are advised as pursues



A. Initial-Deployment Phase

The first step of the proposed TKMP is the initial-deployment phase, during which mobile nodes are assigned specific identities (IDs). In this phase, an appropriate identity is assigned to every Cluster Member (CM), Base Station (BS), and Cluster Head (CH). Since the CH plays an important role in wireless network communication, initial deployment is performed after the mobile nodes have been clustered. After the network model is clustered, multiple CHs are established.

During the initial phase, the predefined network key Nkey is assigned to every node, CH, and BS in the wireless network. The cluster based wireless network has its parameters for everybeginning of communication. The network generally employs a 128-bit network key for secure transmission. The proposed work uses homomorphic encryption to generate the network key.

B. Key Creation Process

After assigning identities to the cluster nodes, the next major stage is to generate keys for the CM, CH, and BS. The key creation stage generates private and public keys for communication among the mobile nodes. This paper acknowledges the PC Encryption Scheme inferred in [22] for making the private and the open keys for the portable hubs. The means

received by PC technique for key age are clarified as pursues:

Consider the kth mobile node in cluster network which starts the correspondence and it needs both the open key and the private key for the correspondence reason. Basically, the root hub makes two separate enormous prime numbers p and q. At that point, the creationC = pq is calculatedamong the random numbers p and q. The private key is determined using Carmichael's function,

$$\lambda(n) = lcm(p-1)(q-1) \quad \text{eqn. (1)}$$

The rest factoris calculated as,

$$r_p^{(p-1)/2} = -1(modp)\ r_q^{(q-1)/2} = -1(modp) \quad eqn.\ (2)$$

Public Key Generation: For creating the public key, the rest factor r and the product C are used. Thus, the public key consists of (r, C).

Private Key generation: The private key is constructed based on (p, q).

The preceding steps are applied to generate the private and public keys for the CM, CH, and BS. The key created for CM, CH and BS is given as follows:

$$[CM^{r}_{key}, CM^{P}_{key}] = \mathrm{PC}(p_1, q_1) \quad eqn.\ (3)$$
$$[CH^{r}_{key}, CM^{P}_{key}] = \mathrm{PC}(p_2, q_2) \quad eqn.\ (4)$$
$$[BS^{r}_{key}, BS^{P}_{key}] = \mathrm{PC}(p_3, q_3) \quad eqn.\ (5)$$

Equation (3) represents the Cluster Member (CM), equation (4) for Cluster Head (CH) and equation (5) for Cluster Head (CH). Where, (p1,q1), (p2,q2) and (p3,q3) are group of large distinct prime numbers stated for the CM, CH and BS, respectively.

C. Key Validation and Confirmation Process

The final phase of the proposed TKMP performs key validation and confirmation. This stage describes the communication procedure between the source and destination mobile clusters during key validation and confirmation. Preceding exchange a verified packet over the correspondence arrange, it is basic to make a secured path for communication among the CM. The secure path between the sender and receiver is established during the key-validation stage before packet transmission. For every data transmission, the TKMP generates a session key that is used to produce the ciphertext.

Begin the data transmit: Packet transmission begins at the source node, and the packet contains its identity (ID), network key (Nkey), and code.

$$APK_{xy} = \begin{bmatrix} Enc(Pid) & Enc(Rid) & Enc(Sh^{xy}_{jey}) \\ Message & Message & Message \end{bmatrix} \begin{Bmatrix} Packet_1 \\ Packet_2 \\ Packet_M \end{Bmatrix} \quad eqn.\ (6)$$

where, Pid indicates the packet identity, Rid indicates the identity of the receiver node refers to the shared key createdamong the origin and the target node. The function Enc()determines the encryption, which is finished utilizing the improved PC calculation with the help of the session key session. The session key is one of the noteworthy components in the proposed TKMP. The session key is generated temporarily and remains valid for the message session between nodes x and y. The following equations describe the encryption performed using the enhanced PC technique.

$$\mathrm{Enc}[P_{id}] = PC(P_{id}, \mathrm{session}^{+}_{key}) \quad eqn.\ (7)$$
$$\mathrm{Enc}[R_{id}] = PC(R_{id}, \mathrm{session}^{+}_{key}) \quad eqn.\ (8)$$
$$\mathrm{Enc}[Sh_{id}] = PC(Sh^{xy}_{key}, \mathrm{session}^{+}_{key}) \quad eqn.\ (9)$$

After the sender establishes the session key, the receiver performs the corresponding operation and identifies the source attempting to communicate through the secure link. The TKMP permits packet transmission only after establishing an authenticated data path (link). For this message, the receiver verifies the authenticity of the source by generating ciphertext. Essentially, the collector makes the ciphertext C1. The ciphertext C1 is generated from the intermediate packet MP. The center bundle MP relies upon the unscrambled data with the session key, and it relies upon the accompanying condition,

$$MP = \left[\begin{matrix} Dec(Enc(Pid)|session^{+}_{key}(recevied)| \\ \left(Enc(Rid)|session^{+}_{key}(recevied)|||Dec(Enc(Pid)|Sh^{xy}_{key}(received))\right) \end{matrix} \right] \quad eqn.\ (10)$$

Where, the session key established by the receiver, and Dec() specifies the decryption done on packet entities based on the received session key.

Generation of ciphertextC1 and C2 can be referred as the security layer 1.

C1= hash(MP) eqn. (11)

The ciphertext C2 is generated using ciphertext C1. The network key provides the next security layer, and consequently C2 is generated as follows:

C2 = [Dec(Enc(C1)|Nkey)||CHpkey] eqn. (12)
C*2 = [(Enc(C1)|Nkey)||CHpkey] eqn. (13)

After generating C2, the receiver responds to the sender's request by transmitting ciphertext C2.Thus, TKMP verifies the packet through multiple security levels, thereby reducing the possibility of security compromise. The sender verifies the integrity of the receiver by comparing the calculated ciphertext C2* with the ciphertext C2 generated by the receiver. When the two ciphertext values match, i.e., C2* = C2, the sender considers the receiver valid and initiates the data transmission. If the ciphertext values do not match, the message is terminated and the session key created for that message is discarded.

Algorithm 1: TRUSTED KEY MANAGEMENT PROTOCOL (TKMP)

IntializeCH,CM,BS.
Process
Step 1: Allocate Nkey to CM, CH and BS using improved PCalgorithm.
Step 2:For each CM, CH and BSand Generate Key Creation using equation 3,4 and 5
End for
Step 3:Execute encryption above the Pid, Rid, and Shared key
Step 4:Start packet transmission and updates Active Profile Key using eqn, (6)
Step 5:Calculate Cipher Text using eqn. (11) & (12)
Step 6:Origin Node finds has(MP*) and C2* correspondingly.
Step 7: ifC2* = C2 then
startpacket transfer
else
State the yth mobile node as the malicious
endif

CONCLUSION

The primary objective of this work is to introduce a Trusted Key Management Protocol (TKMP) for improving secure communication in cluster-based wireless networks. The TKMP is specifically designed for the clustered network and consists of three phases: initial deployment, key creation, and key validation and confirmation. The proposed TKMP employs homomorphic encryption based on the Paillier cryptosystem (PC) for generating the encryption key. In addition, the proposed method develops a geometrical model using verified parameters such as a hashing function, homomorphic encryption, profile key sequence, and random number functions to support authenticated data transmission.

REFERENCES

R. Jayaprakash and B. Radha ,“CBPPRS: Cluster Based Privacy Preserving Routing Selection in Wireless Networks”, International Journal of Engineering &Technology, 7 (3.12) (2018) 439-443.

R. Jayaprakash and B. Radha ,“LBCPR: Load Balancing Cluster Based Privacy Routing In Wireless Networks”, International Conference on Recent Trends in Automation (ICRTA-2018).

L. Zhou, Z. J. Haas, “Securing ad hoc networks”, IEEE Network, Vol. 13, No. 6, Nov. 1999, pp: 24 – 30

Y. C. Hu, A. Perrig, “A survey of secure wireless ad hoc routing”, IEEE Security & Privacy Magazine, Vol. 2, No. 3, May-June 2004, pp: 28 - 39

Y. C. Hu, A. Perrig, D. B. Johnson, “Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks”, in the Proc. Of 8th Annual International Conference Mobile Computing and Networking (Mobicom 2002), ACM Press, 20002, pp. 12-23

M. G. Zapata, N. Asokan, “Securing ad hoc routing protocols”, in the Proc. Of ACM Workshop on wireless security (WiSe), ACM Press, 2002, pp: 1-10

K. Sanzgiri et al., “A secure routing protocol for ad hoc networks”, 10th IEEE International

Conference on Network Protocols, 2002, 12-15 Nov. 2002, pp: 78 - 87

Azarderakhsh, Reza, Arash Reyhani-Masoleh, and Zine-Eddine Abid, "A key management scheme for cluster based wireless sensor networks," Proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, vol. 2, pp. 222-227, 2008.

Udaya, D., Suriya Rajkumar, and Rajamani Vayanaperumal, A leader based monitoring approach for sinkhole attack in wireless sensor network, J. Comput. Sci., 2013, vol. 9, no. 9, pp. 1106–1116.

Xun Yi, Russell Paulet, Elisa Bertino, "Homomorphic Encryption and Applications," Springer Briefs in Computer Science, 2014

Q. Jiang, S, Zeadally, J. Ma and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," in IEEE Access, vol. 5, pp. 3376-3392, 2017.

Bhajantri, Lokesh. (2018). A Comprehensive Survey on Data Aggregation in Wireless Sensor Networks. International Journal of Computer Sciences and Engineering. 6. 798-802. 10.26438/ijcse/v6i7.798802..

J. Choi, J. Bang, L. Kim, M. Ahn and T. Kwon, "Location-Based Key Management Strong Against Insider Threats in Wireless Sensor Networks," in IEEE Systems Journal, vol. 11, no. 2, pp. 494-502, June 2017.doi: 10.1109/JSYST.2015.2422736

Priyanka Ahlawat, Mayank Dave,An attack model based highly secure key management scheme for wireless sensor networks,
Procedia Computer Science,Volume 125,2018,Pages 201-207,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2017.12.028.

