Conditional Key Pre-Distribution with Collaborative Authentication in Wireless Mobile Network

J. Santhosh
Assistant Professor, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India.

Sisha V A
M.Phil Scholar, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India.

Abstract – The Wireless Mobile Network [WMN] is an infrastructure less, self-configuring and dynamic typological oriented network. The unique features of Wireless Mobile Networks including dynamic topology and open wireless medium, may lead WMN to suffer from many security vulnerabilities. To afford a best possible route for secure data transmission, the system introduces a new secure routing protocol. The new authentication mechanism with trust routing protocol "CKPD-AODV" (Conditional Key Pre-Distribution) enables the route discovery with acknowledgement generation mechanism. Based on the trust, Conditional Key Pre-Distribution [CKPD] generates and disperses unique security key for all participants, this frequently verifies the keys and authenticates the hops for data transmission. In previous research works, various researchers proposed packet marking techniques to depict and prevent unauthorized access and data misbehaves. But, still those systems are suffering from huge communication overhead due to its huge key size. So, in this proposed Conditional Key Pre-Distributions (CKPD) authenticates the hop and data by using small key size. This is performed with a acknowledgement schemes, where different types of acknowledgments are generated based on the attack. The major category is ACK and SACK. The SACK indicates the packet about the negative or security issues. The single bit key verifies the data at every hop and retransmits the key with updated one. Using the key size and route information, the system authenticates every hop in the network. Combining the authentication, acknowledgement and collaborative functions, the proposed system gained better result.

Index Terms – Wireless Mobile Network, security, Authentication, Trust calculation.

1. INTRODUCTION

Past few years, have witnessed a rapid escalation in the field of mobile computing due to proliferation of inexpensive, widely available wireless devices. Thus, it has opened vast opportunity for researchers to work on Ad Hoc Networks. In a WMN, nodes within one another's wireless transmission range can communicate directly; however, nodes outside one another's range have to rely on some other nodes to relay messages [1]. So a multiple hop scenario arises. The multi hop scenario is where numerous intermediate hosts relay the packets sent by the source host to make them reach the destination node. WMN is one that comes together as needed, not necessarily with any support from the existing infrastructure or any other kind of fixed base stations [2]. An ad-hoc or general mobile network as an self-ruling system of mobile hosts (MHs), sometimes it serve as a server and routes the data (also serving as routers) connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary communication graph.

This is in contrast to the well-known single hop cellular network model that supports the needs of wireless communication by deploying cluster Heads (CHs). In these radio networks, communications between two mobile nodes completely rely on the intermediate nodes, which are in infrastructure oriented network. In a WMN, no such infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move.

The WMN is very easy to use and at the same time, it is also cost effective one. But, its infrastructure less Environment paves way for challenging security problems. The most important problems in WMNs are secure routing in presence of selfish or adversarial entities which drop the packets they agreed to forward; and in doing this selfish or adversarial entities can disrupt the network traffic and cause various communication problems, Congestion attack which access data illegally, flooding packets and making the network to vast working time. Several research works have been proposed to provide secure route discovery and detection and prevention of attacks. Each one has its own limitations and constraints. Many existing solutions address ways to provide security using cryptography and/or trust based security are presented in the literature covered in [3].

The primary objective of the research is to perform the secure data protection to reduce the data misuse and packet lost using CKPD-AODV protocol. It verifies the hops and path using lightweight method, so data attack decreases and there by increases the packet delivery ratio and reduces energy consumption, End-to-End delay and packet lost. The proposed work is analyzed and simulates in the software Network Simulator-2 (NS2) and compares its effectiveness with the

existing protocol. The simulation will cover different network scenarios with varying network performance parameters such as Packet delivery ratio, Packet lost, End-to-End delay, and Energy Consumption.

2. PROBLEM DEFINITION

Early research works [4][5][6] assumed a friendly and co-operative environment and focus on problem such as simple routing, multihop routing and wireless channel access. At present, security has become a primary concern to provide secure, protected communication between nodes in a potentially hostile environment. Furthermore, distinctive feature of WMNs present a new set of security challenges. Several researchers aim at securing the routing messages of existing routing protocols such as AODV and DSR etc. and they proposed solutions based on cryptographic mechanisms to make routing protocol secure, however, this mechanism require a key management service to keep track of key and node binding.

The key size is huge and very complex at the time of verification. Also it needs a trusted entity called the certificate authority (CA) to issue public key certificate for every node in the network. This is "hard security" mechanisms and too expensive for WMNs. As a result, the system was motivated to develop a trust based secure routing protocol for WMNs. The objective of carried out research work is to propose routing protocols and techniques for secure route discovery and maintain it by preventing different attacks, thus ensuring the transfer of data packets over the network safely. In detail the objectives can be laid down as below:

- Proposed routing protocol to provide secure route discovery and maintenance to prevent collusion, flooding, congestion, and Sybil and DoS attacks.
- Propose a new architecture based on AODV proactive routing protocol to enhance security feature and efficiency.

Secure data transmission in WMN is a challenging task due to its wide variety of attacks. As per the literature, there are several types of attacks interrupts data transmission in Ad hoc networks, but only few algorithms and protocols have been developed to get rid of those attacks. In order to provide secure routing and data authentication, the proposed work has been introduced. Recently, key management is observed to provide better results on the security against those attacks.

These key management schemes can protect the data and authenticates group communications. But, the major problem of key management in the ad-hoc network is the security of the group communication. This research proposes a new trust based protocol for effective secure route discovery of WMN.

3. PROPOSED FRAMEWORK

Many protocols have been designed and implemented to provide secure routing and data transfer [7][8][9], which ultimately results in too much overhead and routing load in the network. Keeping this in view, the CKPD-AODV is proposed and implemented to eliminate unwanted computational and processing overheads that degrade the network. The CKPD-AODV provides a good packet delivery ratio by choosing highly secure nodes, based on trust to establish an authenticated route, thereby enabling secure data transfer.

- A new trust key management scheme which protects the data from collusion, intrusion and man in middle attacks has been proposed.
- Proposes a lightweight single bit key based packet marking technique for fast attack detection. The key generation is created

In this scheme, the nodes in the network are made to fall into one of the three categories; the trusted list, normal list, blacklist, based on the degree of acknowledgements. The acknowledgement generation process involves the grouping of the nodes in the network, based on the parameter called the Acknowledgement (Tscore). Based on the level of the security needed for the data, the nodes in a specific security level are made active for routing, depending on their trust value.

This scheme use single bit key management technique. Trust is compromised, only if secure neighbors are not available. In this case, the route is established by choosing the nodes in the next lower level. Simulation results show that the proposed CKPD-AODV has a better performance than the existing protocols such as OLSRv2 and AODV, in terms of the packet delivery ratio and end-to-end delay, both in the absence and presence of the collusion and congestion attack.

Network construction and route discovery

The first module is initial network construction with 50 mobile nodes. The system simulated the proposed scheme by using the ns-2 network simulator. In the simulation, 50 mobile nodes are placed within a square area of 1500 m × *15*00 m. this use Random Mobility model to determine movements of mobile sensor nodes. In the Random mobility model, each node moves to a randomly chosen location with a randomly selected speed between a predefined minimum and maximum speed.

After reaching that location, it stays there for a predefined pause time. It then randomly chooses another location after that pause time and moves to that location. This random movement process is repeated during a simulation time. The CKPD-AODV provides a proactive way to protect the data from different attacks. So this initially detects the best path based on its previous reputation score. The initial route discovery has the following process.

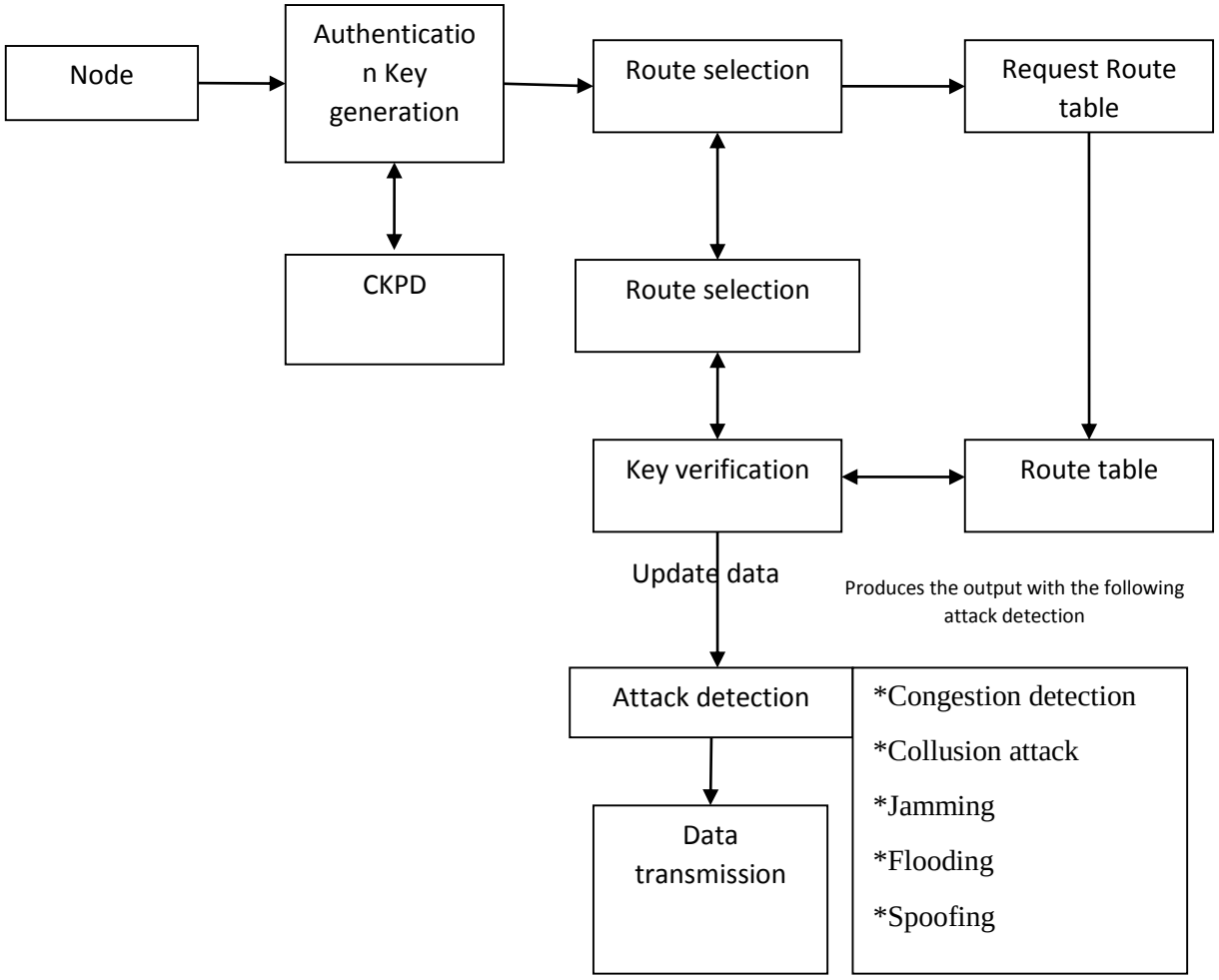

Figure 1.0 CKPD-AODV architecture

RREQ: CKPD-AODV routing protocol is based upon distance vector and uses destination numbers to determine the freshness of routes along with the security constraints. CKPD-AODV is capable of both unicast and multicast routing. CKPD-AODV requires hosts to maintain only active routes, for example the route used to forward at least one packet within the past active timeout period. When a host needs to reach to destination and does not have an active route, it broadcasts a route request (RREQ) packet, which is disseminated in the network.

RREP: A (RREP) route reply is replied back to the source of RREQ to establish the route in the network. It uses HELLO message to determine the connectivity among the neighbors.

Trust Value Verification: In proposal implements CKPD module and reputation scores on existing AODV routing protocol. A trust level of network is defined on the bases of previous behavior of the node.This process initially evaluates trust value of each node by a real number *T* with a continuous value between 0 and 1. In this proposal, trust is described by two mechanisms: direct observation trust and indirect observation. These components are similar to those used in existing systems. In direction observation trust, an observer estimates the trust of his one-hop neighbor based on its own belief. So, the trust value is the expectation of a subjective probability that a trustor uses to decide whether a node is reliable and legitimate.

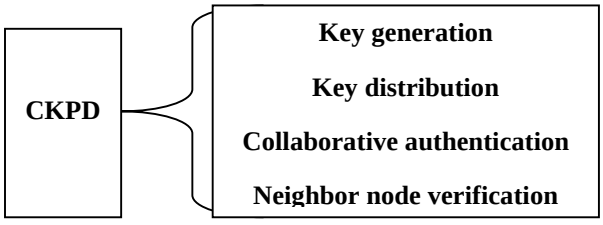

Figure 2.0 Authentication score calculation using CKPD

Direct observation based acknowledgement generation:

As stated on the fig 3.3 the CKPD-AODV evaluates acknowledgements with direct observation on different attacks and different behaviors of node at the time of each attack. For example the proposed system handles flooding attack, congestion attack and collusion attack and other type of interruptions. In the first step in acknowledgement generation with direct verification each observer can overhear packets forwarded by an observed node and compare them with original packets so that the observer can identify the malicious behaviors of the observed node. So the observer node can generate acknowledgement values of its neighbors.

4. CONDITIONAL KEY PRE-DISTRIBUTION (CKPD)

The Conditional Key Pre-Distribution describes the new way of implementing cryptography mechanism to secure routing in WMN. The CKPD itself provide the authentication key and routing information to all the nodes in the transmission path. Few modifications have been made in traditional AODV protocol to done to provide trust aware secure data communication.

The CKPD-AODV is able to find a secure route and if more than one route exists satisfying the required security attributes then it will choose the shortest among them. If insecure route exist between source and destination, then a authentication key is initiated to generate a secure route directly or with intermediate nodes using acknowledgement. The proposed mechanism is also capable of handling the following two cases:

1: Joining a new node in ad hoc network and trust relationship is zero.

2: A CKPD provides acknowledgement, which helps to find the trusted path.

3: disseminates acknowledgement and attacker information to the nearest nodes, which helps to protect the data loss.

A. Authentication Key Generation

The system performs key generation scheme for secure data transmission. This helps to prevent the data from attack. The second module creates an authentication key based on node analysis. In the key generation process, keys are generated dynamically using local time and neighbor details. The CKG algorithm works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key, this makes the CKG algorithm a very popular choice in signature generation.

B. False Information Filtering

Finally the false data will be filtered and malicious node will be blocked based on the key identification. If the key size is greater than the threshold, then the data has been considered as malicious. The data will be dropped further.

C. Trust estimation and acknowledgement verification module

This module compares the collected data with the predefined threshold value and finds the deviation. Based on the information collected and compared by the user, it calculates the direct trust value and stores it into the local database. The direct trust value is calculated mainly based on the behavior of packet forwarding, dropping and tampering. The indirect trust value is determined based on the information collected from other users in the network and maintained by the common database.

D. Neighborhood monitoring and authenticating process

This module proposes a mechanism to detect any control or data attack that results from dropping, delaying, modifying, or fabricating of packets. This module allows a node to distinguish between its neighbors to prevent identity spoofing among them. This is used to build a data structure of the first-hop neighbors of each node and the neighbors of each neighbor. The data structure is used in local monitoring to detect malicious nodes and in local response to isolate these nodes. The message receiver should be able to verify whether a received message is sent by the node that is verified or by a node in a particular group.

The adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected. The proposed message authentication scheme performs a single bit key updating and appending process. The main idea is that for each message *m* to be released, the message sender, or the sending node, generates a source message authenticator for the message *m*. The generation is based on CKG. In order to provide effective authentication against unauthorized data accessing each node in the network member is required to compute and add their signature for all other members who transmits the data in the network.

5. IMPLEMENTATION AND RESULTS

This performed simulations using network simulator. The simulator is written in C++ and implements the code in TCL. The proposed design is implemented using NS-2 and it is analyzed by considering certain parameters like Packet lost, Packet delivery ratio, Energy consumption and End- to-end delay. In the proposed CKPD-AODV framework selects the best path to reduce the packet misuse problems by several attacks and Packet lost and there by increases the packet delivery ratio and energy consumption. Programs in *NS-2* are scripted in OTcl and results of simulations can be visualized using the Network Animator (NAM) and Xgraph.

- This contains a NAM trace file which is abbreviated as data.nam for use with the Network Animator Tool. The following is the sample nam files in the ns2.

```
n -t * -s 0 -x 725 -y -150 -Z 0 -z 40 -v circle -c
black
n -t * -s 1 -x 638 -y -296 -Z 0 -z 40 -v circle -c
black
n -t * -s 2 -x 958 -y -472 -Z 0 -z 40 -v circle -c
black
n -t * -s 3 -x 1116 -y -483 -Z 0 -z 40 -v circle -c
black
n -t * -s 4 -x 1194 -y -518 -Z 0 -z 40 -v circle -c
black
n -t * -s 5 -x 944 -y 209 -Z 0 -z 40 -v circle -c black
```

Figure 3.0 Sample nam file

A Trace file, NS2 also contains the trace fils, which is used for all analysis. This has the .tr extension the following is the sample trace file.

```
M 18.50000 5 (353.56, 455.65, 0.00), (600.12, 480.55),
300.00
M 18.50000 9 (733.09, 145.95, 0.00), (450.85, 400.85),
300.00
M 20.10000 51 (149.00, 613.00, 0.00), (352.83, 100.92),
300.00
v 25.300000000000001 eval {set sim_annotation {Node
Mobility Region setting}}
s 35.100000000 _20_ AGT --- 0 cbr 256 [0 0 0 0] ------
[20:1 17:0 32 0] [0] 0 0
r 35.100000000 _20_ RTR --- 0 cbr 256 [0 0 0 0] ------
[20:1 17:0 32 0] [0] 0 0
s 35.100104005 _20_ RTR --- 1 DSR 32 [0 0 0 0] ------
```

Figure 4.0 Sample trace file

6. PERFORMANCE COMPARISON BASED ON KEY METRICS

The proposed work is successfully implemented using Ns2 simulator. The performance of this proposed work CKPD-AODV using CKPD scheme and new crypto scheme is compared with the existing approaches. This considered the verification delay and authentication key creation delay for deployed data on the WMN in the process of retrieval. Route information retrieval and key generation and verification delay are specified below.

Table 1.0: Comparison of data size

Route information retrieval Process	Delay if Number of nodes (50)	Delay if Number of nodes (100)
Existing System	8.4	14.9
Proposed system	3.6	6.7

Table 1.0 compares the existing and proposed methods in the form of data size. The Route information retrieval delay has been compared. The existing system need more time to perform in 50 nodes. This is very high when comparing with the existing system.

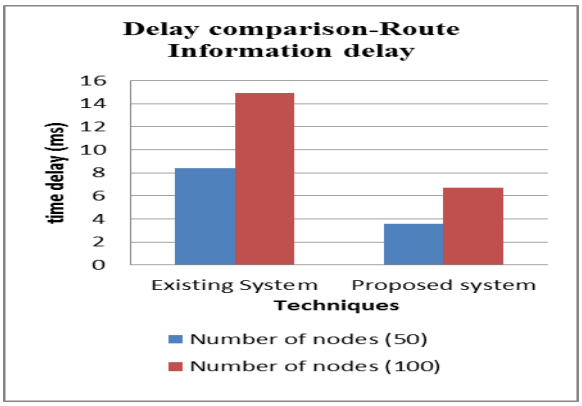

Figure 5.0 Delay comparison chart

The above delay comparison chart indicates the execution time for the algorithm to produce cipher texts and corresponding keys before storing the data. Verification and decryption delay are specified below.

Table 2.0: Comparison of key verification process

Key verification Process	Hop count(10) Delay in (ms)	Hop count(30) Delay in (ms)
Existing System	32.4	78.9
Proposed system	31.6	69.7

Table 2.0 compares the existing and proposed methods in the form of key verification process. The key verification delay has been compared. The existing system need more time to perform 10 users authentication. This is very high when comparing with the existing system.

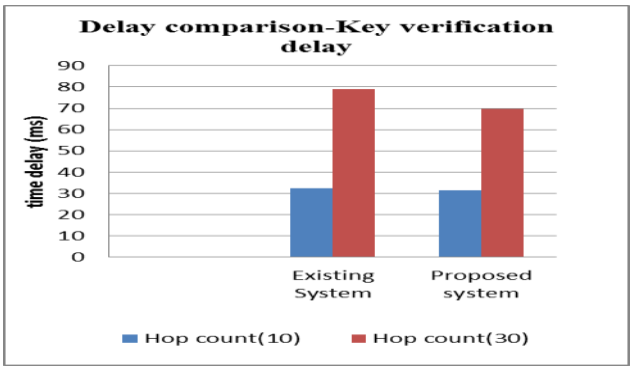

Figure 6.0 Key verification delay comparison chart

The above delay comparison chart indicates the execution time for the algorithm to produce a trust key and verifying at each node. In this paper, initially the qualitative comparative study of proposed protocol with existing technique has been done. Then, after the addition of security to these protocols, the performance of the secure version of the WMN Routing protocol - AODV was analyzed using NS-2 Simulator. Using this, it has done comprehensive simulation results of Average End-to-End delay, energy consumptions, and packet delivery ratio over the routing protocols CKPD-AODV by varying network size and simulation time.

7. CONCLUSION

The system proposed a new secure trust based routing protocol named as CKPD-AODV protocol against different type's attacks in the WMN such as flooding attacks, congestion attacks and collusion attacks. Especially, the approach effectively prevents the data from potential damages due to data attackers and this also protects data by using modified CKG cryptographic function. In order to measure the risk of attacks and data authentication at each hop has been carried out with single bit key verification. This system extended the work of pinpointing the attacker node to their neighbors. Based on several metrics, this system is investigated the performance and other security approach and the experiment results clearly demonstrated the effectiveness and scalability of this proposed CKPD-AODV mechanism approach. The proposed work also integrated the acknowledgement scheme for fast attack analysis and routing. The pre key distribution and the acknowledgement verification are combined together and improved the network performance.

REFERENCES

[1] Varshney, Upkar, and Ron Vetter. "Emerging mobile and wireless networks." *Communications of the ACM* 43, no. 6 (2000): 73-81.

[2] Malladi, Rajeswari, and Dharma P. Agrawal. "Current and future applications of mobile and wireless networks." *Communications of the ACM* 45, no. 10 (2002): 144-146.

[3] Santhosh, J., and V. A. Sisha. "A Comparative Study on Authentication Schemes for Mobile Networks." *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org* 7, no. 10 (2017).

[4] Jabeen, Qamar, Fazlullah Khan, Shahzad Khan, and Mian Ahmad Jan. "Performance improvement in multihop wireless mobile adhoc networks." *the Journal Applied, Environmental, and Biological Sciences (JAEBS)* 6 (2016): 82-92.

[5] Javidi, Tara, and Eric Van Buhler. "Opportunistic Routing in Wireless Networks." *Foundations and Trends® in Networking*11, no. 1-2 (2016): 1-137.

[6] Uddin, Md Forkan, Catherine Rosenberg, Weihua Zhuang, Patrick Mitran, and André Girard. "Joint routing and medium access control in fixed random access wireless multihop networks." *IEEE/ACM Transactions on Networking (TON)* 22, no. 1 (2014): 80-93.

[7] Mahmoud, Mohamed MEA, Xiaodong Lin, and Xuemin Sherman Shen. "Secure and reliable routing protocols for heterogeneous multihop wireless networks." *IEEE transactions on parallel and distributed systems* 26, no. 4 (2015): 1140-1153.

[8] Tang, Di, Tongtong Li, Jian Ren, and Jie Wu. "Cost-aware secure routing (CASER) protocol design for wireless sensor networks." *IEEE transactions on parallel and distributed systems* 26, no. 4 (2015): 960-973.

[9] Liu, Yuxin, Mianxiong Dong, Kaoru Ota, and Anfeng Liu. "ActiveTrust: secure and trustable routing in wireless sensor networks." *IEEE Transactions on Information Forensics and Security* 11, no. 9 (2016): 2013-2027.