ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

An Elliptic Curve Diffie-Hellman protocol with Dynamic Token Ring based Secure communication in Wireless Sensor Networks

[1]K.S. Dhanalakshmi, [2]Dr. B. Kannapiran, [3]S. Renubala

[1]*Assistant Professorr, Department of Electronics and Communication Engineering.Kalasalingam University, Virudhunagar, Tamil Nadu, India*
[2]*Professor and head of the Department of Electronics and Instrumentation Engineering. Kalasalingam University, Virudhunagar, Tamil Nadu, India*
[3]*PG Scholarand Department of Electronics and Communication Engineering. Kalasalingam University, Virudhunagar, Tamil Nadu, India*

ARTICLE INFO

Article history:
Received 20 January 2015
Accepted 02 April 2015
Published 20 May 2015

Keywords:
Elliptic Curve Diffie-Hellman,An Adaptive Multi –Token,Dynamic Token Ring(DRP) and Wireless Sensor Networks (WSNs).

ABSTRACT

Background: Wireless sensor networks (WSNs) are the important domain for applications that includes critical security causes like monitoring military activities and detection of forest fire. Light-weight IDS handles many kinds of attacks, in this paper Adaptive Multi-Token Approach (AMTA)based secure authentication system that uses variant of Elliptic Curve Diffie-Hellman (ECDH) protocol along with Dynamic Token Ring (DRP) based MAC protocol for wireless sensor network is proposed. It also deals with intra-flow and inter-flow contention problems in MAC layer with the help of a Dynamic Token Ring (DRP) based MAC protocol for wireless sensor networks. It is called dynamic, since the token ring in a cluster can be a low-priority ring or a high priority ring. The node can join high priority ring dynamically according to transmission status. Obtained simulation results show that DRP protocol has superior performance in improving data delivery efficiency and avoiding collisions. The proposed approach will provide a solution for inter-flow/intra-flow contention problems as well as hidden/exposed terminal problems. **Objective:** The main objective of this paper is to proposes a new location based rewarding system, where node can collect location-based tokens from token distributors, and then reuse their collected tokens at token collectors for beneficial rewards. A security and privacy responsive location which is based on rewarding protocol to the system that portrays the limits and reliability of the process. **Results:** The proposed approach provides lesser overhead, Average overhead and dropped packet for selfish node with better packet delivery ratio and Latency than the existing Trust theory. **Conclusion:** In this multi-token Authentication system an efficient and secure data transmission in sensor networks is obtained, this shows that the proposed secure transmission method reduces computation and communication overhead.

To Cite This Article: K.S. Dhanalakshmi, Dr. B. Kannapiran, S. Renubala, An Elliptic Curve Diffie-Hellman protocol with Dynamic Token Ring based Secure Communication in Wireless Sensor Networks. ***Aust. J. Basic & Appl. Sci.,*** *9(16): 188-196, 2015*

INTRODUCTION

Broadcast communication protocol is used by sensor nodes in wireless sensor networks, where the sensor signals are used to analyze the sensed environment. Sensor nodes are small in size that sense events, process data and communicate with one another to send information. Sensor networks are used for variety of applications that includes military sensing and tracking, environment monitoring, patient tracking and smart environments, etc. When a sensor node is depending on small battery to function it may require working for a long duration. Hence the sensor operations like communication, computation and sensing, whose energy efficiency needs to be optimized. The energy required to transmit particular information is inversely proportional to exponential of the transmission time. When sensor network are deployed in a hostile environment, security becomes more important as they prone to different types of malicious attacks. For instance, an adversary can easily listen to the traffic and impersonate one of the network nodes. The characteristics of security are authentication, integrity, privacy, non repudiation and anti-playback. Most of the threats and attacks against wireless networks are similar to the wired counterparts. Use of spread spectrum modulation techniques, effective power control and directional antennas helps to prevent the detection of transmission signals.

- Cryptographic methods can be used to protect the information being transferred.

Corresponding Author: K.S. Dhanalakshmi, Assistant Professor, Department of Electronics and Communicationn Engineering, Kalasalingam University, Virudhunagar, India.
Tel: +91 9003964091 E-mail: dhanalakshmi.jai3@gmail.com

For a considerable number of smart meters a key management scheme was designed by *NianLiu,et al*. The design of key management scheme is related with the various mode of transmission, they are unicast, broadcast and multicast. The normal network traffic in an AMI systemis not affected by the distribution of the keys its related data .*Jia-Lun Tsai, et al* proposed a Elliptic Curve Digital Signature Algorithm. In addition, we also showthat the proposed scheme can support identity revocation and trace. A verifier (RSU or OBU) can determine that a received signature has been generated by a revoked vehicle depending on this security property. The proposed scheme is safe against well-known attacks, this can determined by security analysis.A polynomial-based scheme is a symmetric- key based implementation which was said by *Jian Li, et al*, while this is based on ECC, which helps to obtain a hop by hop message validation built- in threshold of the polynomial-based scheme without any weakness. we then proposed a hop by hop message authentication model based on the SAMA. *Hangyang Dai et al*, implemented a algorithm on new key pre distribution based on matrix-based technique that was proposed and numerically evaluated . The node capture technique that hasrigid resilience and large network connectivity can be achieved by an Elliptic Curve Digital Signature Algorithm that helps to authenticate all broadcast messages, which was proposed by *Yongsheng Liu et al*. Thus, the broadcast messages for the signature of overhead are meant to be accounted. This scheme maintains high security that is so rigid as conventional PKC based broadcast authentication schemes beyond low overhead.*GildasAvoine et al* suggested an *analysis* of privacy-friendly authentication protocols devoted to RFID that are based on well-established symmetric-key cryptographic building blocks; require a reader complexity lower than OSK/BF. Some protocols, such as O-RAP, O-FRAP, and OSK/BF, cannot withstand timing attacks.*Yun Li et al*..devised some criteria to quantitatively measure SLP for routing-based schemes. The quality of the message is obtained through content encryption, it is difficult to adequately address source-location privacy. The SLP protection methods for WSNs source-location information leakage in routing can be measured. *TaekyoungKwon et al.*. Constructed two levels of chains that have definite intervals and cross-authenticate each other, which is called as X-TESLA. Through this the short key chains are continued indefinitely and new interesting strategies and management methods are made possible. It also significantly reduces unnecessary computation and buffer occupation, and leads to comprising solutions to the problems.X-TESLA buffer for long interval of upper levels by making the nodes to wait, in which the packets that are entering into the system are eliminated due to the buffer limit.*Muhammad Adnan Tariq et al*... proposed a new approach to provide authentication and privacy in a pub/sub system which has broker-less content. This approach is highly scalable based on number of subscribers and publishers in the system and the number of keys maintained by them. Hence Private keys are assigned to publishers and subscribers, and credentials are marked in the cipher texts.*Pathak, et al* proposed an efficient and secures routing protocol to find out the single and cooperative black hole attack. It encloses a feasible trust based solution that examines the trustworthiness of neighboring nodes. This nodes keeps misbehaving nodes aside from being a part of a network communication process.*Khalifa,et al* gave a security method for WSN, that relays on protecting the transport and application layer on CMAC message authentication and AES encryption. The overhead obtained in the RTP was not addressed by this method . *Kumar and Patel* discussed a secure and Energy efficient data dissemination protocol for WSN. In this method, the information is passed to BS by CH using session key.This scheme defend against attacks on routing protocol that attract traffic by advertising high quality routes to BS.*Mao*demonstrated a secured mechanism for data collection in WSN. This approach protects the datain WSNs from the malicious nodes. A key based secure routing algorithm and counter based intrusion detection algorithm detects malicious node. *Rajendiran, et al* implemented a novel approach to attain efficient and secure key-pre distribution technique in WSN. A seed key was used in an elliptical curve, which assigns priority to sensor node. The private key ring for each sensor node was generated using the point doubling mathematical operation over the seed key. A link was established between two nodes by sharing the private key *Yeh, et al* depicted an Elliptical Curves Cryptography (ECC) secured authentication protocol, which offers high security in WSNs. This scheme prevents the network from various attack namely, insider and Masquerade. This mechanism was vulnerable to forgery and replay attacks.To address such protection challenges, Intrusion Detection System (IDS) is necessary to sense the malicious attackers before they can accomplish any significant damages to the network. Here the key encryption is complete at every node to increase the performances against contemporary approaches.

Subhasis Dash,Azeem Ahmad et al Single token creates the one time authentication when the communication of node takes place, so there are many opportunities for the attacker node to hake the information. Because of this above reasons there will be loss of energy. But in comparing with Single token system, Multi token there will be many numbers of authentications and also inter node communication takes place, so there is less opportunities for the attacker node to hake the information and also there is no loss in energy in Multi token system

The rest of the paper describes as follows Section II describes the detailed description of the Trust based secure routing protocol. Section III shows the nature of proposed method. Section IV gives performance analysis and Section IV concludes the paper.

Trust based secure routing protocol:

S.Renubalaet al.... The existing method involves a novel fuzzy with trust based secure model routing protocol (FTPR). This method reduces the energy consumption by avoiding malicious node. It also shrinks the number of recommendation collected from neighbors to compute indirect trust. This method reduces packet loss by recognizing and rejecting malicious nodes based on the trust value. Here, the trust of the neighboring node is predicted based on direct trust, number of trust fluctuation and recommendation inconsistency. The existing system prevents the network from the black-hole attack, bad mouthing attack and contradictory behavior. A trust evaluation model is considered by the behavior of dynamic nodes in the open environment and manipulating features of nodes trustworthiness. The trust value is calculated by utilizing the Analytic Hierarchy Process and this value offers a prediction of one's future behavior. The existing method uses the fuzzy logic to calculate the trust of the nodes. These values are compared with the threshold value. The trust value above the threshold is considered as trusted nodes and the packets are passed through the node. The trust value below the threshold value is termed as un-trusted node.. This system can be protected by dynamic replaying routing information from severe attacks that can damage WSN. It also produces high resilience scalability, high throughput and less energy consumption .

A.Fuzzy logic:

Fuzzy if-then rules have been applied to much application such as control systems, decision making, pattern recognition and system modeling. The if then rules is being used to check the following parameters which includes energy level of the node, Bandwidth, communications of the node, collision acquiring and also it will check the connections of the node. The algorithm of fuzzy rule-based inference consists of three steps, namely,

- Fuzzy matching- calculates the degree to which the input basic steps and condition of the fuzzy rules
- Inference- calculates the rule's conclusion based on its matching degree.
- Combination- combines the conclusion inferred by all fuzzy rules into a final conclusion.

By considering the above parameters the trust value is calculated for the network using fuzzy logic. In order to obtain a secure routing mechanism in WSNs.

There are some drawbacks in this existing system which can be overcome by proposed method. The drawback is as follows:

- In our existing research we use five different types of rule based security system; we have multi number of iteration for check each and every rule on each node.
- Because of using these five different rules, there will be checking takes place each time so there is high delay and high energy consumed

Adaptive multi-token approach:

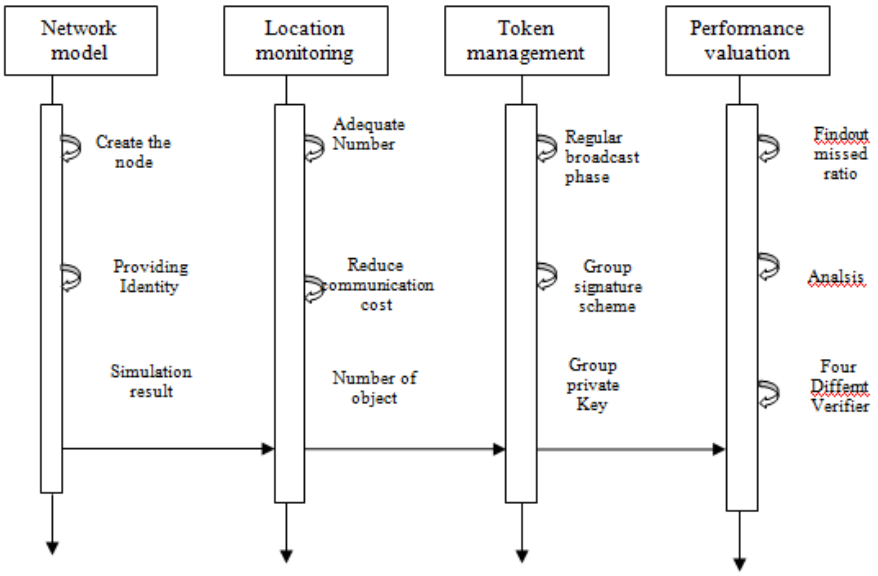


Fig. 1: An overall Sequence Diagram of the proposed An Adaptive Multi Token approach for secured communication in Wireless Sensor Networks(WSNs)

Fig.1 shows the overall Sequence Diagram for proposed an Adaptive Multi-Token Authentication mechanism for secured communication. Two neighbor nodes can be authenticated through secure token by agreeing on a secret key. By this method we can determine user's identity and it also helps to assure that the recipient is from the source that it claims to be from. In order to create and choose a constituent security provisioning method, so that the security services can be implemented which also helps to reduce the performance network degradation which is caused by enhancement of security, we tried to provide the optimal tradeoff between the sufficient security provisioning and the affordable network performance degradation through a systematic resource-aware self-adaptive security provisioning approach. It also deals the intra-flow and inter-flow contention problems in MAC layer with the help of a Dynamic Token Ring (DRP) based MAC protocol for wireless sensor networks. It is called dynamic, since the token ring in a cluster can be a low-priority ring or a high priority ring. The node can join high priority ring dynamically according to transmission status. Our simulation results show that DRP protocol has superior performance in improving data delivery efficiency and avoiding collisions. It is a good solution for inter-flow/intra-flow contention problems as well as hidden/exposed terminal problems.

In our multi-token Authentication method we have realized an efficient and secure data transmission in sensor networks. Fig.2 shows the flow for proposed Multi–Token Adaptive mechanism for secured communication. We show that secure transmission method tends to reduce overhead communication and computation significantly and it can be used in on the shelf sensor platforms practically. Two neighbor nodes can be authenticated through Secure token by agreeing on a secret key. By this method we can determine user's identity and it also helps to assure that the recipient is from the source that it claims to be from. In order to create and choose a constituent security provisioning method, so that the security services can be implemented which also helps to reduce the performance network degradation which is caused by enhancement of security, we tried to provide the optimal tradeoff between the sufficient security provisioning and the affordable network performance degradation through a systematic resource-aware self-adaptive security provisioning approach. Therefore, minimal continuous security services will be given for WSN in synergistic and adaptive manner. WSN is liable to defects like selfish node and compromised node attacks which is also called as insider attack, which is caused by insufficient resource limitation and absence of physical protection. Due to lack of trust among nodes, the true protection for upper protocol layer (e.g., network layer and transport layer) is not received from lower layer protocol (e.g., MAC layer and data link layer and) that delivers hop-by-hop security protection. This security coverage is called as "blanket security coverage". Conventionally, network security counter measures are provided statically, e.g., a maximum level of security service.WSN systems network operation leads to the unnecessary waste of network resource when no attack is launched when this type of static total security provisioning solution is un affordable by the resource scarce. If the unprotected attacks occur the WSN network cannot be secure, when only economic security solution is provided for cost saving purpose and very limited security protection is provided. In protocols like 802.11 MAC which are contention based, each multi-hop data flow encounters contentions not only from the transmissions of itself, but also from other flows that bypassing the neighborhood.

Advantages:

- Less memory usage,
- Less delay (No iteration)
- Less energy consumed

Network model:

Providing identity for each node in the Network the simulations were run with 200 nodes randomly distributed in an area of 1500 m x 1500 m. To increase the confidence of the results, a simulation result was obtained by using different seeds averaging over 20 runs.

Location monitoring:

The objective of this step is to provide security that each sensor node identifies an adequate Number of objects to compute a network area .The communication cost is reduced by relying on a heuristic that some have not determined the required objects in specified number, the messages received by the sensor nodes only are forwarded to its neighbors.

Token management*:*

The communications can be classified into two different phases. They are, the key distribution phase and the regular broadcast phase. The network condition and geographic messages are sent periodically by nodes in the continuous phase as they get keys dynamically in the key distribution phase. A group consists of one group public key and many group private keys.

C. Elliptic Curve Diffie-Hellman (ECDH) Protocol:

A shared key is created by ECDH protocol between two parties. Some public information is exchanged between two parties. Using this public data and private data these parties determines the shared secret key. Moreover, some third party, cannot access to the private details of all devices, and will not be able to analyze the shared secret from the

accessible public information. This work proposed the Diffie-Hellman algorithm using elliptic curve cryptography. During secret communications over a public network a shared secret key is used which was made by Diffie – Hellman, that can be used for exchanging data. Moreover, it's widely used with technical details of internet security technologies, such as TLS and IPSec to deliver secret key exchange for private communications.

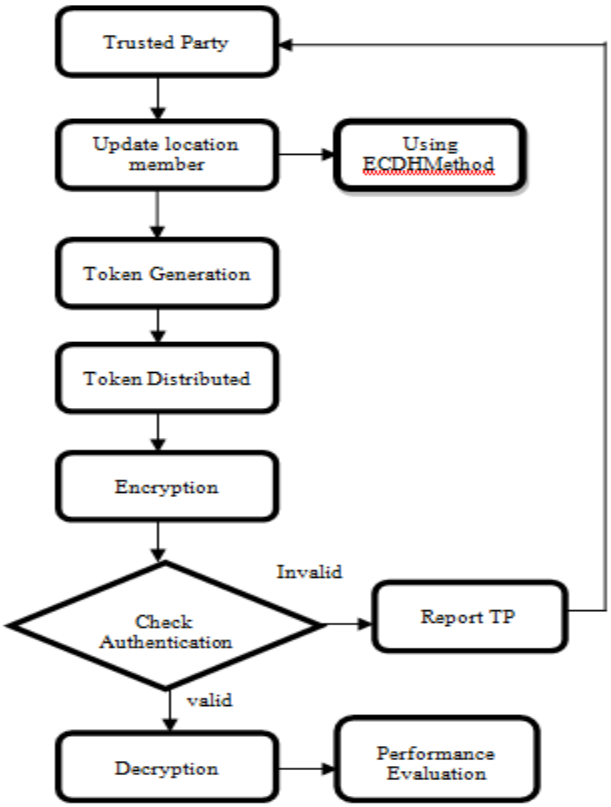


Fig. 2: An overall flow of the proposed for An Adaptive Multi -Token basedsecured communication in Wireless Sensor Networks (WSNs)

For example, the key part of the process is *A* and *B*, which exchange the secret key. This process creates an identification key, which is reverse for additional party. In addition, their sent and received data is encrypted and decrypted by a common secret key A and B. In this research work, the Diffie-Hellman algorithm is based on the multiplicative group modulo *p*, when the EDCH protocol is based on the elliptic curve group. Initially, base point *P (a, b)* of order *n* is selected on the elliptic curve *C* and defined over the field *XY (p)*.

- The user *U* choose a random number $s_u \epsilon [2, n-2]$ and after computing$Q_u = s_u P$, and sends it to the server *S*.
- Then, the server *S* choose a random number $s_s \epsilon [2, n-2]$ and after computing$Q_s = s_s P$, sends it to the user *U*.
- Subsequently, receiving Q_s the user *U* calculates the key$E_U = s_u\, Q_s = s_u s_s P$.
- After receiving Q_U the server *S* calculates the key$E_s = s_S Q_U = s_S s_U P$.
- In addition, both the user and server have the similar key$E = E_S = E_U$.

The ECDH provides a slight change that the recognized value can be pre-determined by the user and made to flow through the server. The protocol can be improved for sending a secret value from the server to the user.

Key Broadcasting:

The ECDH key agreement protocol is responsible for the generation of private/public key. The concatenation of these key results is broadcasted in the WSN. The equivalent node starts to send the packets to the existing nodes in the network, when the key is checked to be a valid key. When the key is not effective, the packets are eliminated and the status is sent to base station (BS).

Performance analysis:

Simulation Environment:

The proposed An Adaptive Multi-Token protocol has been simulated in NS2.The simulation parameters are shown in table 1.To have a detailed Secure communication-related information over a simulation, the ns-2 code is modified to obtain the amount of energy consumed (Secure communication

spent in transmitting, receiving) over time. In this way, the accurate information is obtained about energy at every simulation time.

Table 1: Simulation Parameters.

Simulation Area	870 X 870 in meters
Number of Nodes	200
Transmit range	40 m/sec
Simulation Time	100 m/sec
Key Size	1024bytes
Packet Size	512 bytes

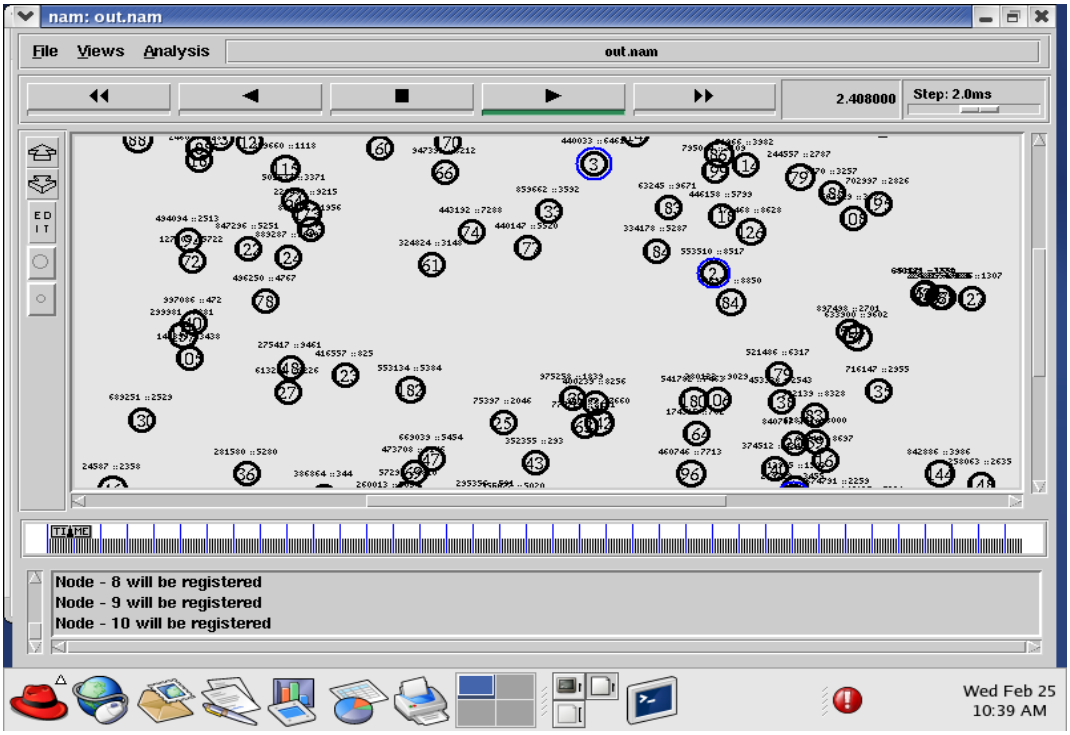
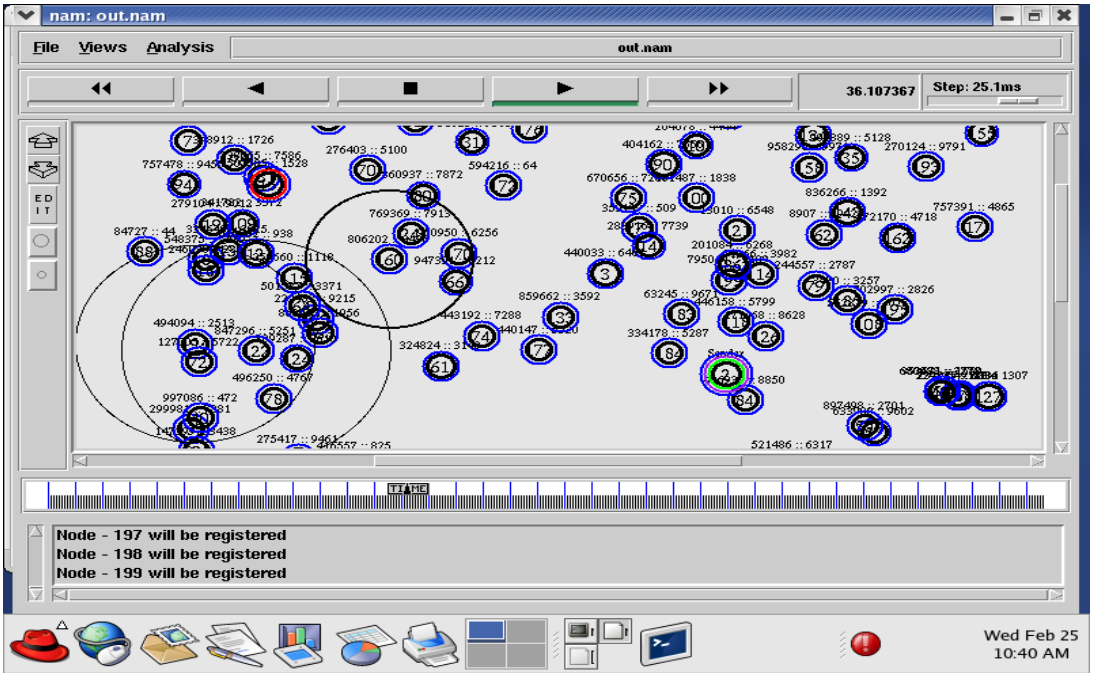


Fig. 3(a): Node deployment.



(b)

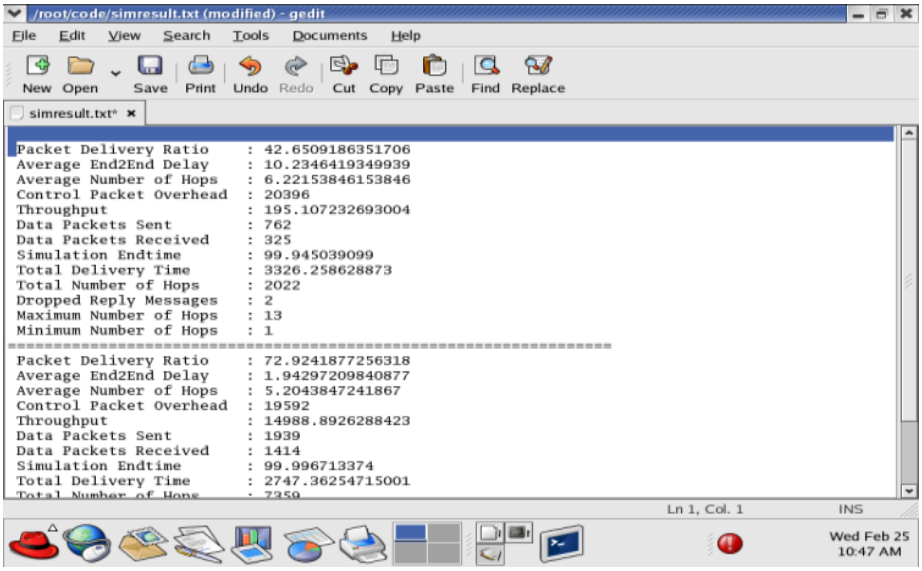


Fig. 3: (b) Registration of node with BSFig.3.(c) Simulation Result.

The fig.3 explains the overall steps involved in the proposed approach. Fig.3a shows the formation of network where the network comprises of 200 nodes numbered from (0-199). The nodes in the network register with the Base Station (BS) node. The nodes are registered to initiate the communication process which are shown by fig.3a, the nodes generates the reports to the BS, where the communication is established. Fig.3b shows the trustworthiness of the node and key generation. Fig 3c shows the Simulation Result achieved by using Adaptive Multi-Token approach by BS.

B.Simulation Results:

The following metrics are used to evaluate the performance of the secure communication protocol being proposed. The value for table 2 describes Packet delivery ratio and Average Latency for Trust and Token based approach. The value for table 3 describe Average dropped and Avera.ge overhead for Trust and Token based Approach. The metrices such as average delay, packet loss, packet delivery ratio, energy consumption.

Table 2: PDR and Average Latency for Trust &Table 3. Average dropped packet and Average overhead for Trust & Token-based Approach and Token -based Approach.

	Trust- based approach		Multi-Token –based approach	
No Of Selfish Node	Average Dropped Packet	Average Overhead	Average Dropped Packet	Average Overhead
1	0	4	0	4
2	0	5	0	5
3	1.9	9.5	0.9	8.1
4	1.9	11	0.9	10
5	2	15	1	12
6	2	17	1	14
7	2.5	18	1.5	14
8	3.9	18	2.8	17
9	5.2	18	3	17
10	8.5	18	5	17
11	8.5	17	5	17
	Trust- based approach		Multi-Token –based approach	
No Of Nodes	Packet Delivery ratio (PDR)	Average Latency	Packet Delivery ratio	Average Latency
20	80	0.48	98	0.45
40	75	0.46	93	0.37
60	62	0.46	92	0.325
80	58	0.45	92	0.25
100	45	0.425	91	0.2
120	42	0.41	82	0.15
140	32	0.375	82	0.12
160	28	0.36	81	0.1
180	25	0.35	80	0.08
200	15	0.3	78	0.05

C. Comparison Analysis:

Fig. 4 shows the Average Dropped Packet with respect to selfish node for the existing Trust theory and the proposed Multi Token Approach. The proposed methodology has low Average Dropped packet ratio than the existing Trust theory. Fig. 5 shows the Average Overhead with respect to selfish node for the existing Trust theory and the proposed Multi Token Approach. The proposed methodology has low Average Overhead ratio than the existing Trust theory. When the No of Selfish node is differ from Minimum to Maximum number. Fig. 6 describes the Packet Delivery Ratio (PDR) with respect to the simulation time for the existing Trust theory and the proposed Multi Token Approach. The proposed methodology has a higherdelivery ratio than the existing mechanism. Fig. 7 shows the Average Latency with respect to node for the existing Trust theory and the proposed Multi Token Approach. The proposed methodology has low Average Latency ratio than the existing Trust theory.

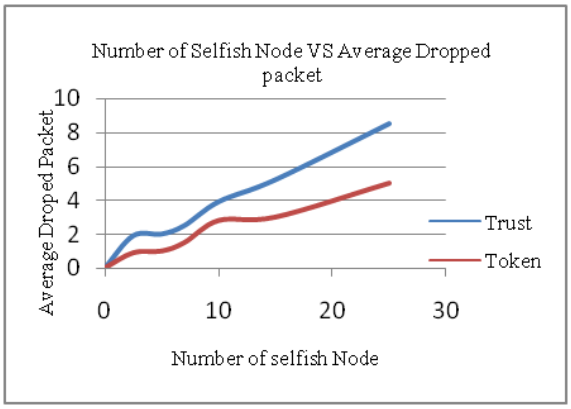


Fig. 4: No. of Selfish Nodes vs Average Dropped packet.

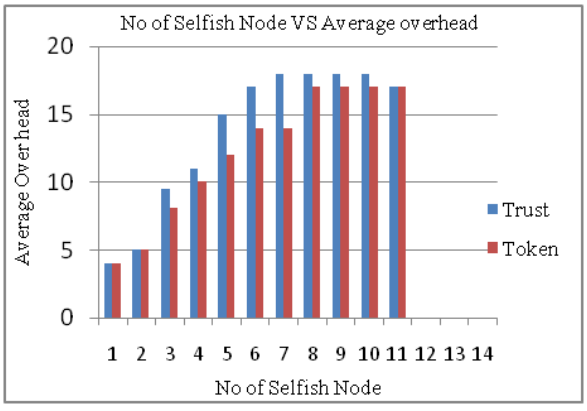


Fig. 5: No. of Selfish Nodes vs Average Overhead.

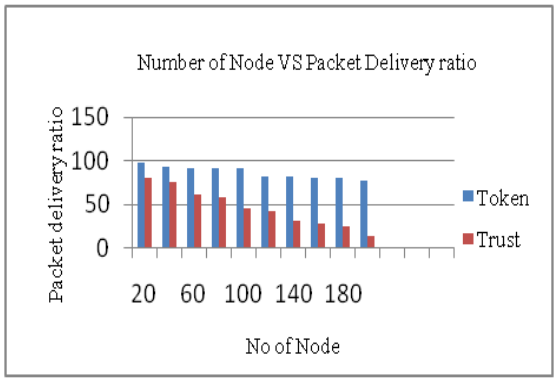


Fig. 6: No. Of Nodes Vs. Packet Delivery Ratio.

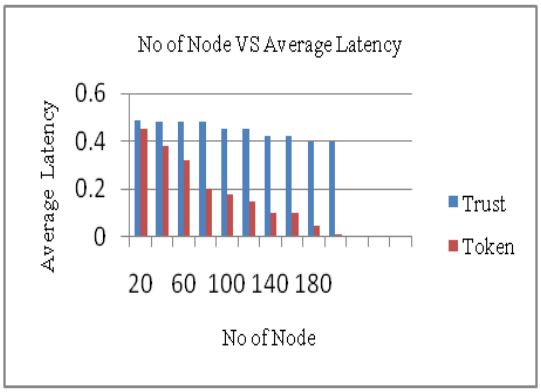


Fig. 7: No.of Nodes Vs. Average Latency.

Conclusion:

This paper has presented Adaptive Multi-token based detection mechanism to safeguard the network against flooding attack and black hole attacks. This paper has presented the identification of threshold exists for the similar justified new nodes and new defected quantities. This paper also proposes the privacy conserving, secure and nominal Token-based rewarding. Which are used to distribute and collect the token. Obtained simulation results show that Elliptic Curve Diffie Hellman protocol along with DRP protocol has superior performance in improving data delivery efficiency and avoiding collisions. This result clearly shows for solving inter-flow/intra-flow contention problems as well as hidden/exposed terminal problems. The proposed approach provides lesser overhead, Average overhead and dropped packet for selfish node with better packet delivery ratio and Latency than the existing Trust theory.

ACKNOWLEDGMENT

We thank the Department of Electronics and Communication Engineering of Kalasalingam University,(Kalasalingam Academy of Research and Education), Tamil Nadu, India for permitting to use the computational facilities available in Centre for Research in Signal Processing and VLSI Design which was setup with the support of the Department

of Science and Technology (DST), New Delhi under FIST Program in 2013.

REFERENCES

Azeem Ahmad, Muhammad Mustafa Hassan and Abdul Aziz, 2014. "A Multi-Token Authorization Strategy for Secure Mobile Cloud Computing", 2nd IEEE International Conference on Mobile Clo Computing, Services, and Engineering, 24(3): 136-141.

Dhanalakshmi, K.S., B. Kannapiran and A. Divya, 2014."Enhancing Manet Security Using Hybrid Techniques' In Key Generation Mechanism ," Electronics and communication system (ICECS),International conference on, 1(5): 13-14.

Gildas Avoine, Muhammed Ali Bingo, Xavier Carpent and Siddika Berna Ors Yalcin, 2013. "Privacy-Friendly authentication in RFID systems: on sublinear protocols based on Symmetric-Key Cryptography" IEEE Transactions on Mobile Computing, 12(10): 2037-2049.

Hangyang Dai and Xu. Hongbing, 2010. "Key pre distribution approach in Wireless Sensor Networks using LU Matrix" IEEE Sensors Journal, 10(8): 1399-1409.

Jia-Lun Tsai, 2014. "An improved cross-layer privacy-preserving authentication in WAVE-Enabled VANETs" IEEE Communications Letters, 18(11): 1931-1934.

Jian, Li, Li. Yun, Jian Ren and Jie Wu, 2014. "Hop-by-Hop message authentication and source privacy in Wireless Sensor Networks" IEEE Transactions On Parallel and Distributed Systems, 25(5): 1223-1232.

Kumar, N., M. Kumar and R. Patel, 2013. "A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks," IJ Network Security, 15(3): 490-500.

Mao, Y., 2011. "A Secure Mechanism for Data Collection in Wireless Sensor Networks" Applied Mathematics & Information Sciences, 25(7): 97-103.

Ming, Li., Sergio Salinas, Li. Pan, 2014. "LocaWard: A Security and Privacy AwareLocation-Based Rewarding System" IEEE Transactions on Parallel And Distributed Systems, 25(2): 343-353.

Muhammad Adnan Tariq, Boris Koldehofe and Kurt Rothermel, 2014. "Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption" IEEE Transactions On Parallel and Distributed Systems, 25(2): 518-528.

Nian, Liu., Jinshan Chen, Lin Zhu, Jianhua Zhang and He. Yanling, 2013. "A key management scheme for secure communications of advanced metering infrastructure in smart grid" IEEE Transactions On Industrial Electronics, 60(10): 4746-4756.

Nour El Din, M.K., M.H. Taha, H.N. Elmahdy and I.A. Saroit, 2012. "A Secure Energy Mechanism for WSN and Its Implementation in NS-2," Wireless Communication, 72(4): 984-990.

Pathak, G.R., S.H. Patil and J.S. Tryambake, 2014. "Efficient and Trust Based Black Hole Attack Detection and Prevention in WSN," International Journal of Computer Science and Business Informatics, 14(3): 222-245.

Rajendiran, K., R. Sankararajan and R. Palaniappan, 2011. "A secure key predistribution scheme for WSN using elliptic curve cryptography," ETRI Journal, 78(33): 791-801.

Renubala, S. and K.S. Dhanalakshmi, 2014. "Trust based Secure routing protocol using Fuzzy Logic in Wireless Senor networks,"IEEE International conference on Computational Intelligence and Computing (ICCIC), 45(99): 1264-1268.

Subhasis Dash, Amulya Ratna Swain and Anuja Ajay, 2012. "Reliable Energy Aware Multi-Token Based MAC Protocol for WSN" IEEE International Conference on Advanced Information Networking and Applications, 43(8): 144-151.

Taekyoung Kwon and Jin Hong, 2010. "Secure and efficient broadcast authentication in Wireless Sensor Networks" IEEE Transactions On Computers, 59(8): 1120-1133.

Yeh, H.L., T.H. Chen, PC. Liu, T.H. Kim and H.W. Wei, 2011. "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," Sensors, 34(11): 4767-4779.

Yingying Chen, Jie Yang, Wade Trappe and P. Richard Martin, 2010. "Detecting and localizing identity-based attacks in Wireless and Sensor Networks" IEEE Transactions On Vehicular Technology, 59(5): 2418-2434.

Yongsheng, Liu., Li. Jie and Mohsen Guizani, 2012. "PKC based broadcast authentication using signature amortization for WSNs" IEEE Transactions On Wireless Communications, 11(6): 2106-2115.

Yun, Li., Jian Ren and Wu. Jie, 2012. "Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks" IEEE Transactions On Parallel and Distributed Systems, 23(7): 1302-1311.