HOP-BY-HOP MESSAGE AUTHENTICATION AND SOURCE PRIVACY IN WIRELESS SENSOR NETWORKS

Ranjini.P [1] *Kathiresan.V*[2]

ABSTRACT

Message authentication is a big challenging task in large scale Wireless Sensor Networks. Most of the existing works depending on the cryptography process or polynomial based schemes, through these techniques can't able to identify the bots in secure communication. Polynomial based schemes set the threshold for each and every large data message communication, so delay factor is high. In my proposed work using the Elliptic Curve Cryptography [ECC] scheme user can send the unlimited messages sharing in secure manner, here introduce the new internal behavior identification scheme name called Awareness Creation Dynamic Caches [ACDC]. Through this form a cache contents in dynamically in clusters. Construct the direct cache communication for node integrity checks. Process gives the high level awareness for each and every communication for clusters.

ECC and ACDC process play the major role in fast and secure and awareness based hop by hop message communication. The proposed system utilizes several techniques to protect, prevent and avoid routing misbehaving attacks. In order to identify and block the nodes which tries to drop or modify the data.

Index Terms— Hop-by-Hop authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy, simulation, Wireless Sensor Networks (WSNs), distributed algorithm, decentralized control.

I. INTRODUCTION

The large scale unlimited size of dense sensor network with thousands of nodes and the need to manage with limited resources and conserve energy as much as possible, on each single node as well as throughout the network, makes secure communication challenging. Wireless communication links and multi-hop message transmission is extremely vulnerable to eavesdropping and manipulation. A node that wants to collect sensor data from distant peers must at least be able to check the integrity of the received data. Such a framework is usually established by an institution that is trusted by both communication endpoints, e.g. a base station (online) or a certification authority (offline). Many applications for sensor networks need only restricted communication modes, such as between nodes and the base station. In that case, security can be supported using the resources available at the base station. Sensor nodes are required

[1]Research Scholar, RVS College of Arts and Science College, Sulur, ranjinipalraj@gmail.com

[2]Assistant Professor, RVS Arts and Science College, Sulur, kathiresan.v@rvsgroup.com

only to have a trust relationship with the base station, which imposes moderate requirements on memory and CPU power of single nodes; the purpose of this paper is to assess the options for protecting the integrity of messages in sensor networks without the need to rely on base stations. The goal is not to have a solution that protects malicious attacks, network routers take the complete knowledge for data communication, before data send our dynamic cache group updates the information about node and network links, so ACDC perform well and make effective communication.

1.1 About Wireless Sensor Network

WSNs were initially designed to facilitate military operations but its application has since been extended to health, traffic, and many other consumer and industrial areas. A WSN consists of anywhere from a few hundreds to thousands of sensor nodes. The sensor node equipment includes a radio transceiver along with an antenna, a microcontroller, an interfacing electronic circuit, and an energy source, usually a battery. The size of the sensor nodes can also range from the size of a shoe box to as small as the size of a grain of dust. As such, their prices also vary from a few pennies to hundreds of dollars depending on the functionality parameters of a sensor like energy consumption, computational speed rate, bandwidth, and memory.

1.2 WSN Applications

Wireless sensor network is designed to perform a set of high-level information processing tasks such as detection, tracking, or classification. Measures of performance for these tasks are well defined, including detection of false alarms or misses, classification errors, and track quality.

Applications of sensor networks are wide ranging and can vary significantly in application requirements, mode of deployment (e.g., ad hoc versus instrumented environment), Sensing modality, or means of power supply (e.g. battery versus wall socket). Sample commercial and military applications include:

1. Environmental monitoring (e.g. traffic, habitat, security)
2. Industrial sensing and diagnostics (e.g. appliances, factory, supply chains)
3. Infrastructure protection (e.g. power grid, water distribution)
4. Battlefield awareness (e.g. mutitarget tracking)
5. Context-aware computing (e.g. intelligent home, responsive environment)

II. Related work

Information-theoretic schemes: In the information theoretic approach defense is handled in an end-to-end manner. Then one can leverage on error correction schemes while letting the intermediate nodes to implement standard network coding operations. In specific some existing system proposed a scheme in which receivers can detect pollution attacks. Later some authors developed the first polynomial time network coding

schemes that tightly achieve the error correction rate bounds. Recently the work in [5] proposed efficient network coding construction to attain the optimal error correction rates in the multiple-source scenarios.

Cryptographic schemes:

In [4] homomorphism hash functions were used to verify the integrity of the packet. However, both of [4] and [5] assumed secure channels to transmit hash values and the homomorphism signature scheme in [6] involves high computational complexity. DanWright Z Metreveli [7] combined hash functions and RSA signatures to detect pollution attacks. However, a recent work [5] proved that this scheme did not satisfy the required homomorphism property. S. Agrawal and D. Boneh, [4] proposed a non-homomorphism signature scheme that used subspace checking to verify the packet. But their scheme requires the source to know the whole file before the transmission.

D. Boneh, D. Freeman. [1] Generalized the scheme in [7] to support data streaming by involving public key signatures for each individual vector. Compared with digital signature schemes, message authentication codes (MACs) are used in [4] and [7] against pollution attacks. However, in [2], the corrupted packet may not be identified at the first hop downstream node and thus it may pollute other packets.

However, RIPPLE requires global synchronization among nodes, which is similar to DART. Although MacSig is an innovative hybrid-key scheme, it still has a large overhead.

In [6], the S. Ganeriwal, L.K. Balzano was proposed to detect the attacker in the intra-flow network coding systems. However, in this scheme, a central entity, the controller is needed to master the complete network topology and then performs the coordination. In [5], they proposed a new defense scheme that is based on the null space properties and it is not relying on any assumptions about the network topology or time synchronization. However, the secure channel among wireless nodes is needed. In [3], S. Marti, T. Giuli, K. Lai, a key pre-distribution based tag encoding scheme was proposed, in which all intermediate nodes and sinks can detect the correctness of the received data packets.

An alternative solution was proposed in [4] to thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial. The idea is to add a random noise, also called a perturbation factor, to the polynomial so that the coefficients of the polynomial cannot be easily solved.

However, a recent study shows that the random noise can be completely removed from the polynomial using error-correcting code techniques S. Ganeriwal, L.K. Balzano [6]. For the public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key [7], P. Michiardi and R. Molva, "A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," [8]. One of the limitations of the public key based scheme is the high computational overhead.

III . P ROPOSED METHODOLOGY

3.1 Proposed System :

Proposed work implements the novel ECC scheme along with **ACDC (Awareness Creation Dynamic Caches)** based authentication scheme for effective attacks detection, recovery and blocking. This allows a node to verify if it's received packets belong to specific rule criteria, we construct the dynamic caches in every clusters, we form a direct communication with every caches, so cache collect and update the cluster node information and transaction information's, ACDC scheme make the overall awareness in large scale secure communications. Our scheme can also provide message source privacy.

Key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key. The recent progress on **Elliptic Curve Cryptography (ECC)** shows that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security resilience.

They scheme that provides hop-by-hop node authentication without the threshold Limitation, and has performance better than the symmetric-key based schemes. The distributed nature of this algorithm makes the scheme suitable for decentralized networks.

Achieving compromise-resiliency, flexible- time authentication and source identity protection, they scheme does not have the any problem. Proposed scheme is more efficient than the polynomial-based algorithms.

3.2 THE PROPOSED SCHEME PROCESS:

- Encrypted key insertion
- Tag creation
- Data forwarding
- Intermediate packet verification
- Dynamic Cache Creation
- ACDC Process

Advantages:

- Delay time minimized.
- Secure all packets
- Delete all unwanted & modifier packets
- minimize the bandwidth

3.3 Contributions Of The Propsoed Work

The system proposing protocol performs set of processes which are helped to effective attacks detection, recovery and blocking nodes. We construct the dynamic caches in every clusters collect and update the cluster node information details. So propose an efficient key management framework to ensure isolation of the compromised nodes. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key. The recent progress on elliptic curve cryptography (ECC) shows that the public-key schemes can be more advantageous in terms of memory usage. While ensuring message sender privacy, ACDC can be applied to any message to provide message content authenticity. Protocol utilizes several techniques to

protect, prevent and avoid routing misbehaving attacks. Order to identify and block the nodes which tries to drop or modify the data has been implemented the Intermediate packet verification algorithm.

III. Implementation Of The Proposed Work

The ACDC protocol performs set of processes which are helped to identify Detecting attacks detection, recovery and blocking nodes in WSN.

Encrypted key insertion: Authentication can be achieved through an especially for elliptic curve Public-key cryptosystems. Elliptic Curve Cryptography (ECC) Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication Generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations.

Key generation: Alice's () public and private keys are associated with a particular set of elliptic key domain parameters (q, FR, a, b, G, n, h). A public key Q = (x, y) associated with the domain parameters (q, FR, a, b, G, n, h) is validated using the following procedure

- Hop-by-hop message authentication
- Message authentication
- Message integrity

Destination List Length (DLL):

Destination List Length (DLL) indicates how many nodes are in the node list, and thus will determine the length of the header.

Packet length: The ACT header size is not fixed since the destination list length is variable. This length includes the standard ACT header.

- **Router ID** - The router ID of the packet's source. In ACT, the source and destination of a routing protocol packet are the two ends of an (potential) adjacency.
- **Area ID** - identifying the area that this packet belongs to. All ACT packets are associated with a single area.
- **Checksum** - The standard IP checksum of the entire contents of the packet, starting with the ACT packet header but excluding the 64-bit authentication field.

Source Address is the address of the source node, which equals the transmitted group ID of this packet, and Destination List Address stores the locations of the DLL destination nodes. In this protocol all the multicast members are included in the packet header. The protocol adopts the following terms defined in the header to describe similar concepts in existing multicast protocols:

- **Batch size** — number of packets in a batch. It has the same value for all packets in a given batch.
- **Forwarder list size** — number of forwarders on the forwarder list. It has the same value for all packets in a given batch.

- **Packet number** — index of the packet in the batch.
- **Forwarder number** — index of the forwarder on the forwarder list. It indicates which node on the list has just transmitted the data packet.
- **Batch map** — an array whose size equals the batch size. Each element of the map is indexed by the packet number, and its value is the forwarder number of the highest priority forwarder that this packet has reached.

When the TTL reaches zero, the request packet is discarded before finding target. Table 1 shows the structure of an MARK header. After a node receives a multicast packet, it then retrieves the destination node list from the MARK packet header. If this node is inside the destination list, it removes itself from the list and passes a copy of the packet to the upper layers in the protocol stack. MARK then checks the TTL value and drops the packets if the TTL is lower than 0.

IV. Experimental Result

4.1 Disadvantages:

A disadvantage of redundant traffic-based methods is the very high overhead incurred by the redundant operations or packets, leading to high cost.

- Existing anonymous protocols map construction leaks destination node locations and compromises the route anonymity.
- attacker can mount traffic analysis based on packet type
- optimality problem
- Need careful design to unlink ability
- difficult to hide information on packet type and node identity
- Computation overhead.

4.2 Proposed Advantages:

4.2.1 Packet Delivery Ratio:

Packet delivery ratio is a ratio between the received packets at the destination and the total number of packets transmitted from the source. When the packet delivery ratio is high then the performance is also high.

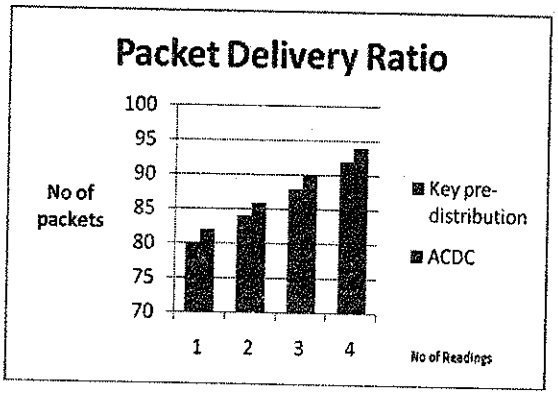

Figure 1: Packet Delivery Ratio

4.2.2 Average End –to –End Delay:

End to end delay is the difference between the packet receiving time and the packet sending time. Average delay is the ratio between the time difference and the total number of packets received at the destination. When the

average end –to –end delay is low then the performance is high.

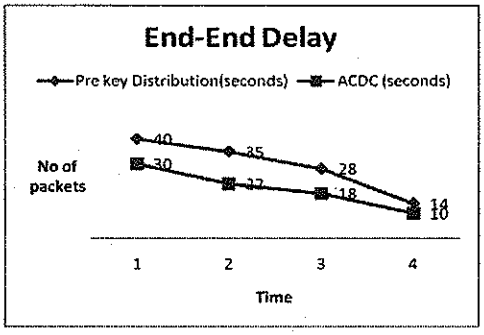

Figure 2: Average End –to –End Delay

The above chart shows that the proposed performance is considerably improved than the existing system. The proposed system gives less delay with the security and privacy.

4.2.3 Time Complexity:

The time complexity of an algorithm is measured as the time taken to execute a method or function by an algorithm for the given input. The time complexity of an algorithm is generally articulated using "big O" notation. Here the time complexity of ACT is O (N) where the complexity is O (N) +4.

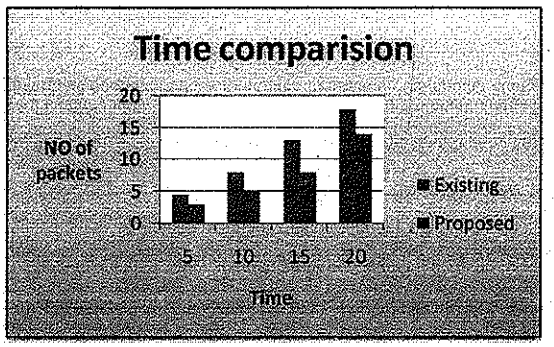

Figure 3: Time Complexity

4.3 Comparative Table:

Comparative Table to compare the values of Packet Delivery Ratio, Delay, Time Comparison for Existing and Proposed values.

4.3.1 Packet Delivery Ratio :

PDR = (No of packets Received / No of packets send) * 100

Table 1: Packet Delivery Ratio

No of Packets	Existing	Proposed
5	80	82
10	84	86
15	88	90
20	92	94
30	96	98

4.3.2 Average End –to –End Delay:

Table2: Delay

Total Packet	Existing time (seconds)	Proposed time (seconds)
90	40	30
80	35	22
70	28	18
50	14	10

4.3.3 Time Complexity:

Table 3: Time Complexity

Time Expected	Existing	Proposed
5	4.5	3
10	8	5
15	13	8
20	18	14

V. Conclusion

The system has proposed can identify misbehaving forwarders and routes that drop or modify packets in wireless Sensor networks based novel **ECC (Elliptic Curve Cryptography)** scheme along with **ACDC (Awareness Creation Dynamic Caches)**based authentication scheme. In order to identify and block the node which tries to drop or modify the data, proposed internal behavior identification scheme algorithm. So this Basic idea behind the proposed system is to identify the direct cache communication for node integrity checks and its value of every node. The proposed scheme quickly detects misbehaving forwarders and routes that drop or modify packets with very small number of efforts and claims. Protocol provides high security level for all kinds of sensor networks and outstanding communication performance and minimal storage Consumption.

VI. Future Enhancement

This proposed system can be extended as performance measurement countermeasures. In this proposed system the security measures are concentrated to achieve data integrity in the network communication. Whenever the security protection systems are involved in the system then the performance must be measured to make sure that the system is giving the best performance speed while working. So, the enhancement work can be as follows,

- To speed up the attacker detection process
- Can propose new idea to measure node performance speed and so on.

References

[1] D. Boneh, D. Freeman, J. Katz, and B. Waters, Signing a Linear Subspace: Signature Schemes for Network Coding. Springer, Mar. 2009.

[2] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, *"Secmr —A Secure Multipath Routing Protocol for Ad Hoc Networks,"* Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, *"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,"* Proc. ACM MobiCom, 2000.

[4] S. Agrawal and D. Boneh, Homomorphism MACs: MAC-based integrity for network coding, in Proc. Appl. Cryptography Newts. Security, 2009, pp. 292–305.

[5] I. Khalil and S. Bagchi, *"MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks,"* Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm '08), 2008.

[6] S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, *"Reputation-Based Framework for High Integrity Sensor Networks, Error-correcting code techniques"* ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, 2008.

[7] DanWright Z Metreveli - ý2012 *"combined hash functions and RSA signatures to detect pollution attacks: A Multi-Dimensional Trust Management Approach,"* Proc. 11th Int'l Conf. Mobile Data Management (MDM '10), 2010.

[8] P. Michiardi and R. Molva, *"Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks,"* Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm. and Multimedia Security: Advanced Comm. and Multimedia Security, 2002.

[9] X. Zhang, A. Jain, and A. Perrig, *"Packet-Dropping Adversary Identification for Data Plane Security,"* Proc. ACM CONEXT Conf. (CONEXT '08), 2008.

[10] K.Ioannis, T. Dimitriou, and F.C.Freiling, *"Towards Intrusion Detection in Wireless Sensor Networks,"* Proc. 13th European Wireless Conf., 2007.

[11] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, *"Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks,"* Proc. Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, 2008.

[12] J.M. Mccune, E. Shi, A. Perrig, and M.K. Reiter, *"Detection of Denial-of-Message Attacks on Sensor Network Broadcasts,"* Proc. IEEE Symp. Security and Policy, 2005.

[13] B. Yu and B. Xiao, *"Detecting Selective Forwarding Attacks in Wireless Sensor Networks,"* Proc. 20th Int'l Symp. Parallel and Distributed Processing (IPDPS), 2006.

[14] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, *"An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in Manets,"* IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.

[15] F. Ye, H. Luo, S. Lu, and L. Zhang, *"Statistical En-Route Filtering of Injected False Data in Sensor Networks,"* Proc. IEEE INFOCOM, 2004.

AUTHORS BIOGRAPHY

Ranjini.P, completed her under graduate degree from Bharathiar University Arts and Science College Valparai and has also completed her post graduate level course M. Sc., at Bharathiar University Arts and Science College Valparai and is currently pursuing her M.Phil in Computer Science at RVS College of Arts &Science, Coimbatore, India. Her area of interest is Advanced Networking.

Kathiresan.V, is an Assistant Professor, Department of Computer Applications (MCA) in RVS College of Arts and Science, Coimbatore. He received his B.Sc., in 2003 and MCA in 2006 from Bharathiar University, Coimbatore. He obtained his M.Phil. in the area of Data mining from Periyar University, Salem in 2007. His research interest lies in the area of Data mining. He got Faculty Excellence Award from RVS College of Arts & Science for the Academic years 2007-08, 2008-09, 2009-10, 2010-11, 2011-12 & 2012-13 consecutively