An Efficient Secured Multicast Routing Protocol for Wireless Sensor Network Using Identity-Based Cryptography and Its Application In Biomedical Research

Sampradeepraj T.[1*], Anusuya Devi V.[2] and Chitra D.[1]
1. Department of Computer Science and Engineering, P.A. College of Engineering and Technology, Pollachi, Tamilnadu 642 002, INDIA
2. Department of Computer Science and Engineering, National Engineering College Kovilpatti, Tamilnadu 628501, INDIA
*sampradeepraj@gmail.com

Abstract
Security in Wireless Sensor Network (WSN) remains a challenging problem because of its resource, computing and environment constraints. Key distribution as well as key management is basic in safe communicating in sensor networks. In this paper, a simple and efficient security algorithm based on Identity-Based Cryptography (IBC) is proposed for WSN. This method uses Random Linear Network Coding (RLNC) over Minimum Connected Dominating Set (MCDS) in On-Demand Multicast Routing Protocol (ODMRP). Hence, the proposed protocol is named as I-RLNMCDS-ODMRP, which delivers multicast data efficiently with secure. This paper, analyze the computation and memory overhead of proposed protocol with respect to time in seconds and bytes respectively also analyzed the security properties. Based on experimental results, it is concluded that the proposed protocol takes less time to compute its necessary parameters for encryption and decryption and also takes less memory to store necessary information of a multicast message. In future, the proposed protocol will be tested with health care application of intra body communication for biomedical sensor networks.

Keywords: Wireless sensor network, Multicast routing, IBC, Network coding, Health care, Biomedical

Introduction

WSN is a wireless network with reasonably numerous sensor nodes to examine environmental or physical circumstances [1]. WSN is at present attaining considerable concentration because of their broad applications like environment observing, building structures monitoring, habitat monitoring, traffic surveillance, information gathering, military sensing, wildfire discovery and pollution controlling, etc [1]. Multicast is similar data transferring to different receivers simultaneously.

Multicasting is a much effective technique that supports group communication against broadcasting. Multicasting applications are meetings and military control actions to multicast planned information [2].

For Multicasting in WSN, network backbone formation, channel capacity and security are some networking issues [3]. To solve these issues three state-of-art techniques were used, they are, (1) Minimum Connected Dominating Set (MCDS), (2) Random Linear Network Coding (RLNC) and (3) Identity-Based Cryptography.

The MCDS is a Connected Dominating Set (CDS) with least cardinality [4]. Finding a least sized CDS is NP-Hard [5]. In real time environment, the virtual backbone of the network as small as possible, in order to decrease the protocol overhead, to save life time, energy consumption and cost of construction etc.

RLNC is emerged promising technique for various applications in wireless networks, which has been applied in multicast routing to improve the network capacity for maximum multicast flows and reduce the multicast traffic in WSN [6]. The output data for a given node is achieved by linearly combining its input data. The coefficients of this linear combination are entirely arbitrary in nature, therefore named Random Linear Network Coding [7, 8].

Identity-Based Cryptography (IBC) is a cryptographic algorithm that derives public keys from user's identities such as email address, Uniform Resource Identifier (URI) and Session Initiation Protocol (SIP) [9].

Intra-body Communication is a novel method which employs the human body as an electrical channel in Biomedical monitoring system for wireless body area network (WBAN) [10].

Motivation and Justification of the Proposed Works: Key distribution as well as key management is the basic for the safe WSN communication. Therefore, improving the effectiveness and key management security is the most significant problem. Due to the nature of open wireless access, it is vulnerable to various attacks including pollution attack, node capture attacks and eavesdropping, etc. Hence, security presents important challenge in WSN. Typical security protocols just offer much ease key management systems for WSNs. Example: TinySec [11] and SPINS [12], which may be insufficient for WSN. Furthermore, when the network size is increased, the communication, computation and storage overhead concepts increase considerably also

network security and connectivity obtain not as good as rapidly. Thus, much efficient key distribution as well as re-keying systems are required to improve the security power of the current security algorithms.

Shamir [9] proposed the approach of asymmetric key cryptography by means of individuality as a public key. Shamir formulated an identity-based signature technique with the help of prevailing RSA algorithm [13], yet it was unsuccessful in constructing an Identity-Based Encryption (IBE) system, that remains to be an unresolved issue for about a decade. Boneh and Franklin [14] were capable to build an encryption system using bilinear maps. This lead to a novel period of study in IBC, throughout several identity-based digital signature systems by bilinear maps. Simultaneously, Cock's [15] presented an IBE system via quadratic residuary and it had been restricted in its WSN applicability since the long ciphers along with slower performance generation, because it was on the basis of a ternary quadratic form. Lastly, Boneh et al [14] presented the short length identity dependent digital signature system in classical cryptography via pairing.

To overcome the drawbacks of traditional ODMRP [16], T.Sam et al [17] proposed RLNMCDS-ODMRP a state-of-art high throughput, high reliable reactive multicast routing protocol by using RLNC over MCDS in traditional ODMRP, which considers the characteristics of WSN without security. Recently, RLNC has emerged as a new communication paradigm in WSN, but RLNC based applications are susceptible to probable malicious actions. Many prime attacks types like pollution attacks, random forgery attack [18] and entropy attacks are particularly relevant to RLNC, as, it occupies packet missing in the WSN [19, 20, 21]. Also, the conventional hash function depended signature systems could remain inappropriate for RLNC, because, in the subsequent encoding process the novel source signatures can be devastated by each encoder, which is performed at each forwarder. It is essential to attain effective message integrity and validity for secure random linear network coding. To address the issue aforementioned, a novel protocol is proposed, which aims to develop efficient and high secure multicast routing protocol. This protocol is considering a simple and efficient security algorithm IBC. It is much easier to use than Public Key Infrastructure (PKI) and it provides a more reasonable balance between security and usability. Thus, IBC have been well-recognized as the much efficient concept to deal with this security issues and it is expected that the proposed protocol can be potentially used for achieving efficiency with high secure.

Outline of the Proposed Work: Overall process of the proposed system is depicted in the Figure 1.Here, an efficient secured multicast routing protocol is presented by applying IBC in RLNC over MCDS on ODMRP for WSN. Computational and memory overhead of the presented protocol is examined based on time in seconds and bytes respectively also security properties for the proposed protocol is analyzed.

Organization of the Chapter: The residual paper is systematized like below: Section 2 converses about encryption standards. Section 3 portrays methodology of the intended scheme. Section 4, discusses about the experimental results of proposed approach. Finally, conclusion about the proposed approach is given

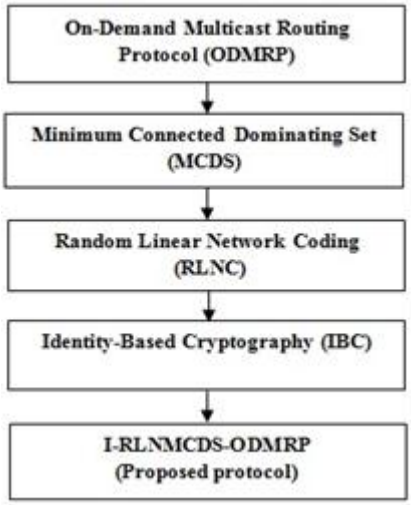

Figure 1: Outline of the proposed work

Related Techniques and Concepts

On-Demand Multicast Routing Protocol: ODMRP is a state-of-art on-demand (reactive) multicast routing protocol [16]. This one is a mesh dependent as well as source intimated algorithm. Forwarding Group (FG) idea is used in developing a mesh structure in a given network also "soft state" approach is followed to maintain a mesh. Figure 2. shows that overview of ODMRP protocol. T.Sam et al [17] given detail explanation about the operation of ODMRP with MCDS.

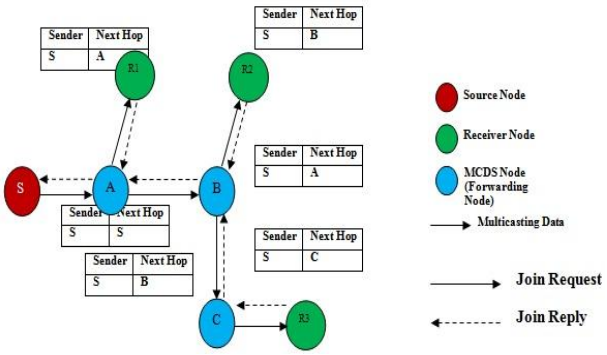

Figure 2: An ODMRP protocol overview

Minimum Connected Dominating Set: The concept of the MCDS appears from the graph theory [22]. It describes a nodes set for a known connected network. The CDS and MCDS network is shown in Figure 3 and Figure 4 respectively. MCDS is constructed from CDS using convex hull. From the definition, a dominating node in MCDS

network has connection with all other network node and they are united themselves also no separate node in the network. In this network, nodes in blue form a MCDS and they are connected through the blue bold lines, which represent the backbone of the network. All other nodes that are marked in white and green node (receiver) can be reached by the blue nodes in the MCDS. In this network, MCDS dramatically reduce the redundant transmissions by sending multicast messages forwarded by MCDS nodes to attain every receivers.

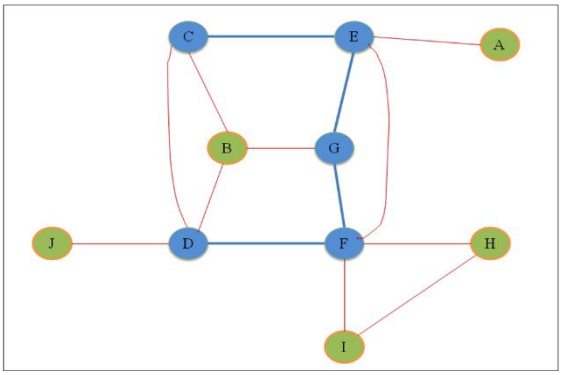

Figure 3. The CDS Network

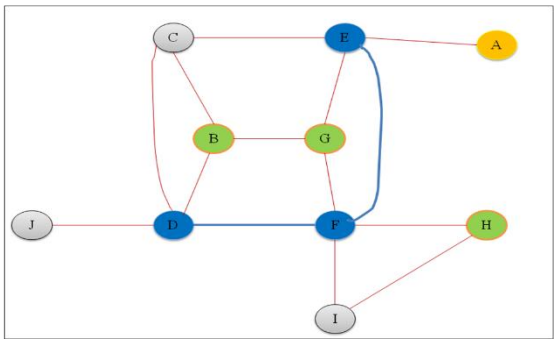

Figure 4: The MCDS Network

Random Linear Network Coding: RLNC is emerged promising technique for various applications in wireless networks, which has been applied in multicast routing to improve the network ability for maximum multicast flows and reduce the multicast traffic in WSN.

In RLNC, the output data for a given node is acquired as a linear input data combination. The coefficients picked for this linear combination are entirely arbitrary in nature, therefore named Random Linear Network Coding. The forwarding node combines packets it has obtained or generated into one or some extrovert coded packets. Typically, RLNC performs three different operations [22], they are 1. Encoding, 2.Re-encoding, 3.Decoding.

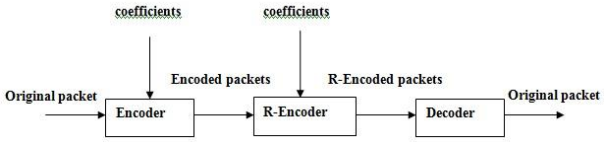

Figure 5: RLNC Process

From the Figure 5, the encoding process can be done at source node of the network. Re-encoding process can be done at forwarding node, which is almost similar to encoding process but the coefficients are completely newly generated. Finally, decoding process can be done at destination nodes. The encoding, re-encoding and decoding operations are implemented via matrix operations.

Review of Encryption standards: The individuality of the sensor node is employed to be the public key in the WSN environment. Therefore, there is no necessitating in binding individuality of a sensor node with its public key for a certificate. As shown in Figure 6, IBC offers realistic public key cryptographic schemes with no complex public key infrastructure usage. IBC seems to be a possible solution for sensor networks in many ways and not required to observe a public key directory, as it is obtained with node individuality which is extensively identified in the network.IBC gives a scalable protection system for that the keys are placed in least. Participating nodes generates a public key for a known node, in case if it has to commune for the primary time. IBC permits each node to transmit safe messages to every the other nodes from the network opening function. No need of earlier interface among the nodes. Information exchange doesn't need any assistance else aid from a third party. Though, identity depended schemes presume the survival of a trusted key production, centre that subjects private keys related to client uniqueness, therefore key distribution is simple.

Adding new nodes to the network is easy in IBC. There is not necessary to change or append new keys to current devices, just add and forward the encryption, therefore new sensor nodes should be programmed with domain features and a private key by the public key producer prior to dispersion. In traditional Public Key Cryptography (PKC) system, adjusted keys are altered using a new private or public key-pair. Considering IBC, key abrogation needs that clients must alter their individuality data which corresponds to known private keys. Most of the authors find that Elliptic Curve Cryptography (ECC) and Rivest Shamir and Adlemen (RSA) are not easy and at times not possible to combine ECC execution with the sensor network application. For example ECC and RSA execution need larger RAM which remains unfeasible to fix on the same sensor node. Table 1 shows IBC in comparison with ECC and RSA based on characteristics, from the theoretical analysis, this paper shows that IBC offers better security than ECC and RSA in WSN.

Table 1
IBC in comparison with ECC and RSA

	Digital certificates	Key directory	Number of Keys	Key distribution	Forward encryption	Non-repudiation
IBC	No	No	N	Simple	Yes	Yes
ECC	No	At each node	O(n)	Simple	No	No
RSA	Yes	At each node and key centre	O(n)	Complex	No	Yes

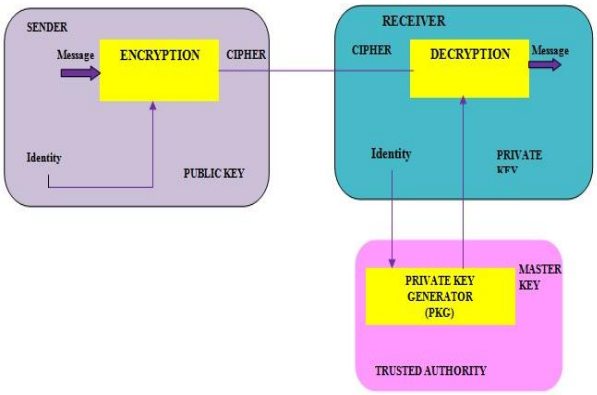

Figure 6: Identity-Based Encryption Scheme

Methodology

ID-based routing technique presented by Lu et al [24]. Multicast routing is the basic functions in WSN that effort to make sure the message delivery from source to destinations. WSN multicast applications are too resource rigorous and need capable multicast routing protocols that poise the energy and time utilization of the whole network, for example remote-sensing functions need the multicast routing algorithms to assist the prompt message deliverence. Normal multicast routing protocol couldn't be exerted straight to a resource conditioned environment of WSN. The secure nature of this proposed protocol depends on the basis of Bilinear Diffie-Hellman (BDH) problem. The network architecture is supposed to be stationary and homogeneous in functions as well as abilities for the proposed model. Here, ID-based multicast routing system, every round has two phases: a set-up phase as well as a steady state phase. Sensor nodes identify at which time every round begins and ceases by synchronization of time. In the proposed system, the timeperiod consumed for multicast message to traverse from the source towards destination nodes are known as T_s then, time needed for message to traverse from normal node towards source node is t_i. The public key is the node's ID linked together to ti (ID + ti). On implementing the ID-based multicast system, every sensor node which wants to confirm them towards another node should attain its private key from anxious PKG. On revocating the node, the source node requires to multicast the compromised node Ids to the sensor nodes, and every node amass the rescinded Ids in a definite round. Prior to distribution, the key-pre distribution phase is carried out in the set-up phase as shown in Figure 7

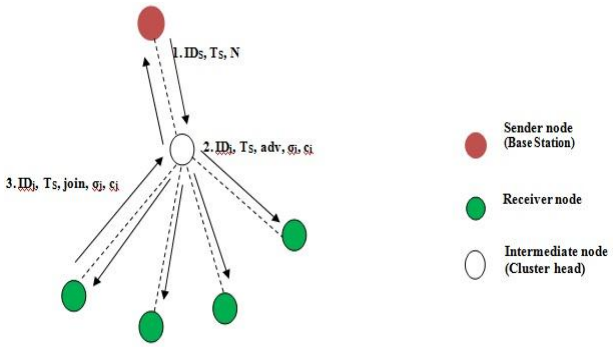

Figure 7: ID-Based Multicast routing in setup phase

Set-up phase:

- Develop public values PP (p, q, E/F_p, G_1, G_2, e) and Let $P \epsilon G_1$.

where p and q are two larger prime numbers then let E be an elliptic curve explained on a finite field F_p. Let G_1 remain a q-order subgroup of the additive group of points in E/F_p then G_2 remain a q-order subgroup of the multiplicative group in the finite filed F_p and e: $G1 \times G1 \rightarrow G2$, which is bilinear map.

- Assume there are 2 cryptography hash functions like H_1 to the point-mapping hash function to map strings towards elements in G_1, then H_2, that maps arbitrary inputs to fixed length outputs, like follows

$H_1: \{0,1\}^* \rightarrow G_1^*$ and $H_2: G_2 \rightarrow \{0,1\}^n$ for some n

- Assume $P_{pub} = \tau P$ as network public key where $\tau \epsilon Z_q^*$ (private key of the PKG)

Preload every sensor node using the public system values PP (p, q, EIF_p, G_1, G_2, e, H_1, H_2, P, τ).

Keep an assumption that source node j needs to multicast a message m. Initially it has its private key to be $d_j = \tau H_1(ID_j||t_i)$, where IDj is the ID of the source node j, then ti is the time stamp of the time interval for the present round from TDMA control. The sensor then obtains an $\alpha \epsilon Z_q^*$ randomly then calculates $\theta = e(P,P)^{\alpha}$. The sensor node further calculates

$c_j = H_2(m||t_i||\theta)$ and let $\sigma_j = c_j d_j + \alpha P$

in which σ_j , c_j forms the digital signature on the message m. the multicast message is recently linked to be in the way of $< ID_j, t_i, m, \sigma_j, c_j >$.

Steady-state phase:

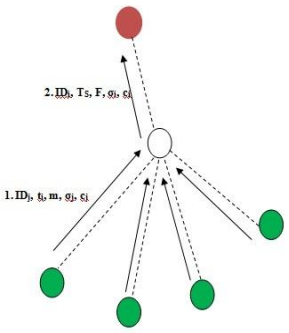

Figure 8: ID-Based Multicast routing in steady state phase

During the second phase, as shown in Figure 8 every sensor node verifies the authenticity, when receiving this concatenated multicast message in the manner as follows: it verifies the time stamp of the present time span t_i and verifies

if the message obtained is fresher. After that, when proper time stamp is present, sensor node further calculates

$$\theta' = e(\sigma_j, P)\, e(H_1(ID_j||t_i), -P_{pub})^{c_j}$$
$$= e(\sigma_j, P)\, e(H_1(ID_j||t_i), -\tau P)^{c_j}$$
$$= e(c_j d_j + \alpha P, P)\, e(H_1(ID_j||t_i), -\tau P)^{c_j}$$
$$= e(c_j d_j + \alpha P, P)\, e(\tau H_1(ID_j||t_i), P)^{c_j}$$
$$= (e(d_j, P)^{c_j}\, e(P,P)^{\alpha})\, e(\tau H_1(ID_j||t_i), P)^{-c_j}$$
$$= e(d_j, P)^{c_j}\, e(P,P)^{\alpha}\, e(d_j, P)^{-c_j}$$
$$= e(P,P)^{\alpha}$$
$$= \theta$$

Then, if $h(m||t_i||\theta') = h(m||t_i||\theta) = c_j$, that equals the one in the received message, the sensor node assumes the obtained message true, then transmits the message towards the following node. In case of failure of verifying process, sensor node assumes the received message is bogus else altered one, can be a wrongly taken one, rejects it. Also the total multicast message packet size at the transmission is equal to $|ID_j|+|t_i|+|m|+|\sigma_j|+|\ h(m||t_i||\theta)|$, in which $h(m||t_i||\theta)$ is a hash value, that is 20 bytes while SHA-1 is made use. $|ID_j|+|t_i|$ are much smaller, which is 2 bytes each, then $|m|$ is considered to be 20 bytes.

The total message size of a transmission packet is $44 + |\sigma_j|$ bytes, in which $|\sigma_j|$ is varying. The elliptic curve E is explained over F_p , the order q of G1 as well as G2 is a 160-bit. Further, p remains an 512-bit prime to obtain high secure stage compared to 1024-bit RSA.

Simulation environment and performance evaluation

Experimental setup: Nodes were positioned evenly at indiscriminate places over an area of 500 m × 500 m in the simulation experiment. The multicast traffic is Constant Bit Rate (CBR) having 250 bytes data packet. The simulation set-ups are generated using the set dest ns-2 with simulation time of 200 seconds. Mobility model employs a random waypoint in a rectangular field. At this time, 1-to-many multicast approach was considered, i.e., Sender is sticked to be one, then receiver may change in span of 9 and 99. The least and greatest speed range between 0 and 20 m/s, correspondingly in pause time interval is 1 simulation seconds, that relates to steady motion as well as transmission rate is 128 Kbps, transmission range is 50 m for all nodes.

Traffic load is fixed as 5 pkts/sec and equally distributed among all senders; arrival rate is set to 10 kbps. Our simulation study shows that the proposed protocol (I-RLNMCDS-ODMRP) using routing metric is SPP. The proposed protocol adopts 80-bit security level (RSA-1024 equivalent) for IBC. The hardware requirement for overhead analysis of proposed protocol is Intel Core-i5-2450M CPU @ 2.50GHz, 4 GB RAM and 32- bit Operating System. The required software is Network Simulator-2.34 (NS-2), VM ware workstation and Windows 7. The simulation parameters are summarized in Table 2.

Table 2
Simulation parameters

S.N.	Parameters	Particulars
1	Simulator	Network Simulator-2
2	Routing protocol	RLNMCDS-ODMRP
3	No. of nodes	varied across 10-100
4	Simulation time	200 secs
5	Simulation area	500 m × 500 m
6	Node movement	Random way point
7	Multicast type	One-to- many
8	Pause time	1 sec
9	Traffic	CBR
10	CBR Packet size	250 bytes
11	Traffic Load	5 pkts/sec
12	Arrival Rate	10 kbps
13	Routing Metric	Success Probability Product (SPP)
14	Transmission rate	128 Kbps
15	Mobility speed	0,5,10,15,20 m/s
16	Transmission range	50 m
17	Topology	Multi-hop
18	Methods	MCDS and RLNC
19	Security Algorithm	IBC (80-bit security level) based on BDH

Performance metrics:

Computational overhead: The proposed protocol requires some computational operations such as initiation, parameter generation, encryption, decryption as well as shared key calculation. Among these, encryption and decryption are the most computationally intensive modules, which require large number of arithmetic operations and performed on large integers.

Storage overhead: Memory consumption can be defined as total number of memory used in bytes for RAM and ROM. The memory amount represents the node ID and to store its parameters for each node. The overhead is more when the value of RAM and ROM is more, then overhead is also more. Storage cost includes the size of both signature generation and verification codes.

Experimental results and analysis: Here, simulation outcomes of the proposed approach for the performance metrics of computation cost and storage cost to execute IBC for WSN are elaborated also security analysis is done.

Computational Overhead Analysis: The empirical computation overhead of I-RLNMCDS-ODMRP is simulated and analyzed with respect to time in seconds in the graph under two criterions: a) By changing the quantity of nodes and b) By changing the node speed, where the security

scheme is developed in five phases: initiation, parameter generation, encryption, decryption as well as shared key computation. The initiation phase with system initiation and configures the necessary libraries. The parameter generation phase entails the selection of random numbers and the computation of ephemeral key. The encryption phase engages the public keys generation and making cipher text of message with keys, while decryption phase involves the making plain text from cipher text. The shared key computation phase entails the shared secret then derives the sharekey computation through the Key Derivation Function (KDF).

Scenario-I – By varying the number of nodes
In the initial condition, the working of proposed protocol is measured for computational overhead (time in seconds) assumed here for WSN by increasing number of nodes from 09 to 99 nodes for constant minimal speed of 0 m/s (static) for network coverage area. The table 3 shows that time taken to compute necessary parameters of proposed protocol.

Table 3
Time costs (seconds) to execute I-RLNMCDS-ODMRP by varying no. of nodes

No.of nodes	Initiation	Parameter Generation	Encryption	Decryption	Shared key Computation	Total
10	1.207	0.012	1.682	1.325	0.005	4.231
20	1.262	0.015	2.246	1.943	0.008	5.474
30	1.361	0.017	2.521	2.223	0.020	6.142
40	1.241	0.210	2.846	2.512	0.024	6.833
50	1.374	0.019	3.200	2.802	0.019	7.414
60	1.281	0.016	3.513	3.013	0.013	7.836
70	1.225	0.014	3.827	3.321	0.007	8.394
80	1.321	0.018	4.173	3.642	0.027	9.181
90	1.262	0.231	4.423	3.851	0.028	9.795
100	1.382	0.224	4.810	4.121	0.026	10.563
Avg	**1.291**	**0.0776**	**3.324**	**2.875**	**0.017**	**7.586**

In average, the proposed protocol consumes 7.5863 seconds to execute for 100 nodes network. It has the most favorable computation difficulty on average and considers that the point multiplication against an elliptical curve (160 bits) with low cost over modular exponential operations of RSA (1024-bits) having similar secure stage. Particularly, during encryption the proposed protocol takes average 3.3241 seconds, to verify and decrypt a multicast message, it consumes 2.8753 seconds. Because, each sensor node only accumulates its specific private key, the key storage work stays stable with network dimension enhancement

Scenario-II – By varying the speed of the nodes: In the2nd scenario, the working of proposed protocol is measured for computational overhead (time in seconds) taken in this section for WSN by improving node speed from 0 to 20 m/s for the constant 20 nodes in network coverage area. Table 4 explains the time taken to compute necessary parameters of proposed protocol.

In mobility scenario, the proposed protocol is used IBC based on elliptic curve digital signature algorithm to ensure secure data transfer by authenticate their identities and establish pair wise keys. The execution time of the proposed protocol is showed in Table 4.

Table 4
Time costs (sec) to execute I-RLNMCDS-ODMRP by varying mobility speed

Mobility speed (m/sec)	Initiation	Parameter Generation	Encryption	Decryption	Shared key Computation	Total
0	1.262	0.015	2.246	1.943	0.008	5.474
5	1.284	0.017	3.511	3.010	0.014	7.836
10	1.223	0.014	3.825	3.323	0.011	8.396
15	1.320	0.018	4.171	3.632	0.027	9.168
20	1.261	0.219	4.313	3.850	0.028	9.671
Avg	1.27	0.0566	3.6132	3.151	0.017	8.109

From the table, analysis shows that the execution time of the proposed protocol varies high when using mobility. It consumes more time (3.6132 seconds) to encrypt a multicast message than decryption (3.1516 seconds) always. In the proposed scheme, encryption involves in two scalar point multiplications with a random 160 bits value with the message. Therefore, a sensor node spends more time for encryption.

Storage Overhead Analysis: The performance of proposed protocol is measured for memory consumption considered in this section for WSN. Table 5 shows that memory consumption of proposed protocol with IBC, ECC and RSA. The memory consumption of I-RLNMCDS-ODMRP of RAM and ROM is 1812 bytes and 11674 bytes respectively, which includes the memory consumption of signature generation and verification code.

Table 5
Memory Consumption in bytes

S.N.	Algorithms (with RLNMCDS-ODMRP)	ROM (bytes)	RAM (bytes)
1.	IBC	11674	1812
2.	ECC	13179	1843
3.	RSA	16384	2150

From the table 5, it is observed that implementation of ECC and RSA with RLNC over MCDS takes so much memory than I-RLNMCDS-ODMRP. Therefore, this may be not possible in fitting all sensor network usage as well as implementing over same node. IBC consumes less memory compared with the ECC and RSA of ROM and RAM since the smaller dimension of system parameters and ephemeral keys. Hence, IBC offers great opportunity to utilize the proposed protocol in the sensor network.

Security Analysis: Here, as shown in table 5 security properties are analyzed for the proposed protocol against traditional ODMRP, ODMRP with RLNC, ODMRP with MCDS and combination of RLNC and MCDS also presented what kind of attacks can be avoided of each protocol as shown in table 6. A safe multicast routing protocol should have preventive measures and should provide superior security over all known attacks. Traditional ODMRP is the most premier mesh based reactive multicast routing protocol and tuned to support efficient and high security in the WSN. The security of the projected protocol appears from the unique way of using identity-based cryptography for different communication types and also from the distinctive manner that the protocol decides the route among a source node and destination nodes

Table 5
Security requirements

Security requirements/ Protocols	Traditional ODMRP	RLNC-ODMRP	MCDS-ODMRP	RLNMCDS-ODMRP	I-RLNMCDS-ODMRP
Data confidentiality	No	Yes	No	yes	Yes
Data integrity	No	No	No	No	Yes
Data authentication	No	No	No	No	Yes
Data freshness	No	No	No	No	Yes
Data availability	No	yes	No	yes	Yes

Observing table 5, it could be said that the presented protocol meets all the security requirements efficiently, but other protocols for WSN are insecure because it does not meet all security properties. Thus, the proposed protocol provides efficiency with high security.

Table 6
Protection against attacks

Protocols	Attacks				
	Wormhole Attack	Spoofing Attack	Blackhole Attack	DoS Attack	Rushing Attack
Traditional ODMRP	Yes	Yes	Yes	yes	Yes
RLNC-ODMRP	yes	yes	Yes	yes	yes
MCDS-ODMRP	Yes	Yes	Yes	yes	yes
RLNMCDS-ODMRP	Yes	Yes	Yes	yes	yes
I-RLNMCDS-ODMRP	No	No	No	No	No

Observing table 6, it is said that the presented protocol provides good security against all byzantine attacks because, it possess all preventive measures against known byzantine attacks by using IBC. Due to the limitations of traditional ODMRP, it requires more security also which increases effectiveness of attack in the absence of defence mechanisms [2, 16]. RLNC permits in-between nodes to mix multicast data from several data flow, hence offers data confidentiality and data availability as an intrinsic level of data security by receiving the same copies at intermediate nodes, but not ensuring data integrity, data authentication and data freshness because of wiretapping and byzantine attacks [6, 20, 25, 26, 27, 28]. In a byzantine attack, the outside adversary is capable to acquire complete control of minimum connected dominating nodes which employed to attack the network from inside, thus MCDS requires more security against all known attacks [4].

Conclusion

In WSN secure multicast routing has been a most important challenge because of node mobility and resource constraint. In this work, Identity-Based Cryptography (IBC) can take part in a critical role in reducing the computational cost as well as memory cost on I-RLNMCDS-ODMRP in WSN. The proposed approach is increased the efficiency of security in the proposed protocol. Based on experimental results, it is concluded that the computational overhead and memory overhead is reduced with respect to time in seconds and bytes respectively in suitable limits evaluated over security level achieved also security analysis shows that the proposed protocol provided better security over all byzantine attacks. As future work, multiple attacks should be considered in the proposed protocol and also the proposed protocol should be implemented in health care application of Intrabody communication for biomedical sensor network.

References

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, A Survey on Sensor Networks, IEEE Comm. Magazine, vol. 40, no. **8, pp. 102-114, Aug. 2002.**

2. Jing Dong, Reza Curtmola, Cristina Nita-Rotaru, Secure High-Throughput Multicast Routing in Wireless Mesh Networks, IEEE Transactions on mobile computing, **Vol.10, No.5, May 2011.**

3. Javad Akbari Torkestani, Mohammad Reza Meybodi, Weighted Steiner Connected Dominating Set and its Application to Multicast Routing in Wireless MANETs, Wireless Pers. Commun., Springer, Feb. **2010.**

4. Du, H., Wu, W., Shan, S., Kim, D., & Lee, W. Constructing weakly connected dominating set for secure clustering in distributed sensor network. Journal of combinatorial optimization**23.2 (2012): 301-307.**

4. Guha, Sudipto, and Samir Khuller. Approximation algorithms for connected dominating sets. Algorithmica **20.4 (1998): 374-387.**

5. R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, Network information flow, IEEE Trans. Inform. Theory, **vol. 46, pp. 1204-1216, July 2000.**

6. P. Ostovari, J. Wu, and A. Khreishah, Network coding techniques for wireless and sensor networks, in The Art of Wireless Sensor Networks, H. M. Ammari, Ed. Springer, **2013**

7. Tracey Ho, Muriel Médard, Ralf Koetter, David R. Karger, Michelle Effros, Jun Shi, and Ben Leong, A Random Linear Network Coding Approach to Multicast, IEEE Transactions on information theory, **vol. 52, no. 10, october 2006**

8. Shamir, A., Identity-based cryptosystems and signature schemes, Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science (Springer-Verlag), **1984: 47-53**

9. C. Karlof, N. Sastry, and D. Wagner., TinySec: A link layer security architecture for wireless sensor networks. 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, **November 3–5, 2004, 162–175.**

10. Mir Hojjat Seyedi, Daniel Tze Huei Lai A Novel Intrabody Communication Transceiver for Biomedical Applications, Springer Nature Singapore Pte Ltd. 2017, series in BioEngineering.

11. A.Perrig, R. Szewczyk, J. D. Tygar, et al., SPINS: Security protocols for sensor networks, Wireless Networks, **8(2002)5, 521–534.**

12. Rivest, Ronald L., Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM **21.2 (1978): 120-126.**

13. Boneh, Dan, and Matt Franklin. Identity-based encryption from the Weil pairing. Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, **2001.**

14. Chiu, W. K., C. Ding, and C. L. Yu. Cocks' IBE Algorithm. **(2010).**

15. S.J. Lee, W. Su, and M. Gerla, On-demand multicast routing protocol in multihop wireless mobile networks, ACM/Kluwer Mobile Networks and Applications, vol. 7, no. 6, **December 2002, pp. 441–452.**

16. T.Sampradeepraj, V.Anusuya Devi, High Reliable-Reactive Multicast Routing Protocol for Wireless Sensor Network, Romanian journal of information science and technology, Romanian Academy (Submitted on Apr **2017).**

17. Johnson, R., Molnar, D., Song, D., & Wagner, D. Homomorphic signature schemes, In Topics in Cryptology—CT-RSA **2002 (pp. 244-262**). Springer Berlin.

18. Heidelberg. Gkantsidis, Christos, and Pablo Rodriguez., Cooperative Security for Network Coding File Distribution, INFOCOM. **Vol. 3. 2006.**

19. T. Ho, B. Leong, R. Koetter, M. M'eard, M. Effros, D. Karger., Byzantine modification detection in multicast networks using randomized network coding, Proceedings of 2004 IEEE International Symposium on Information Theory (ISIT), **2004**

20. S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. M'eard, Resilient network coding in the presence of byzantine adversaries, Proceedings of IEEE INFOCOM, **2007.**

21. D. B. West, Introduction to Graph Theory, 2nd ed. Upper Saddle River, NJ:Prentice Hall, **2001.**

22. Mahmood, Kashif, Thomas Kunz, and Ashraf Matrawy. Adaptive Random Linear Network Coding with Controlled Forwarding for wireless broadcast. Wireless Days. **2010.**

23. Lu, Huang, Jie Li, and Hisao Kameda., A secure routing protocol for cluster-based wireless sensor networks using ID-Based digital signature, Global Telecommunications Conference (GLOBECOM **2010), IEEE, 2010.**

24. R. Koetter and M. Medard, An algebraic approach to network coding, IEEE/ACM Transactions on Networking, **vol. 11, no. 5, pp. 782–795, 2003.**

25. Wu Chi, Huang Cheng, Huang xiaotao, A Combination Scheme against Pollution Attacks in Network Coding, 2012 IEEE/ACIS 11th International Conference on Computer and Information Science.

26. N Cai, RW Yeung, Secure network coding, Proceedings of the IEEE International Symposium on Information Theory (ISIT '02), **June 2002.**

27. Qin Guo, Mingxing Luo, Lixiang Li and Yixian Yang, Secure Network Coding against Wiretapping and Byzantine Attacks, EURASIP Journal on Wireless Communications and Networking **2010**