Opportunistic Routing with Secure Coded Wireless Multicast Using MAS Approach

E. Golden Julie, S. Tamil Selvi, Y. Harold Robinson

***Abstract*—**Many Wireless Sensor Network (WSN) applications necessitate secure multicast services for the purpose of broadcasting delay sensitive data like video files and live telecast at fixed time-slot. This work provides a novel method to deal with end-to-end delay and drop rate of packets. Opportunistic Routing chooses a link based on the maximum probability of packet delivery ratio. Null Key Generation helps in authenticating packets to the receiver. Markov Decision Process based Adaptive Scheduling algorithm determines the time slot for packet transmission. Both theoretical analysis and simulation results show that the proposed protocol ensures better performance in terms of packet delivery ratio, average end-to-end delay and normalized routing overhead.

***Keywords*—**Delay-sensitive data, Markovian Decision Process based Adaptive Scheduling, Opportunistic Routing, Digital Signature authentication.

I. Introduction

In wireless networks multicasting of delay sensitive data is widely used in many applications. Multicasting is the transfer of messages to multiple destinations simultaneously. A common requirement of such applications is that the information must be delivered to as many receivers as possible within certain time constraint [1]. Multicast wireless networks [2] mainly focus on reducing bandwidth and power consumption ensuring secure packet transmission and packet loss detection. In wireless networks, channels are lossy in nature [3] where packets may be lost during transmissions due to reasons such as channel fading [4], [5]. Hence network coding is done to ensure secure transmission. However network coding is susceptible to bogus packet injection attacks in an unfriendly environment. Thus an efficient authentication scheme is required. Secure transmission scheduling is more essential for reducing packet loss in WSN [6]. Digital Signature scheme has been proposed in [7] and [8]. All Scheduling algorithms will not recover the problem of attackers and bogus packet injection [9]. At any time-slot the packet must be transmitted in secure manner is very important in this proposed work.

II. Existing System

Opportunistic Routing in Multihop Wireless Networks has been proposed in [10] to avoid duplication of packets. However the optimal path value for each node with different path was not calculated. In [11] energy efficient Assistant Opportunistic Routing (AsOR) protocol which provides a method for selecting optimal value for each node is proposed. This scheme is not suitable for coded network. Null Key generation [12] to detect bogus packets helps in successfully decoding original packets. But the computational cost is very high for using the null key space properties to defend against pollution attack in wired-coded networks. An efficient key management scheme was proposed in [13] but was not suitable for multicasting delay sensitive data

III. Proposed System

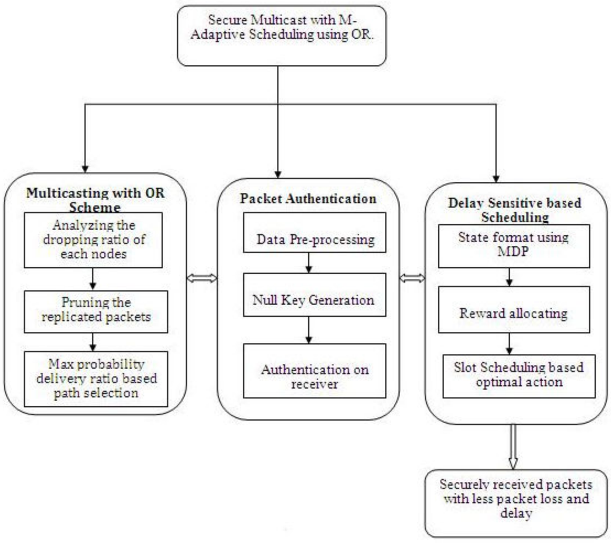
Secure Multicast with M-Adaptive Scheduling using OR.
Multicasting with OR Scheme
Analyzing the dropping ratio of each nodes
Pruning the replicated packets
Max probability delivery ratio based path selection
Packet Authentication
Data Pre-processing
Null Key Generation
Authentication on receiver
Delay Sensitive based Scheduling
State format using MDP
Reward allocating
Slot Scheduling based optimal action
Securely received packets with less packet loss and delay

Fig. 1 Architectural Diagram

Fig. 1 shows the architectural diagram of the proposed protocol. Multicasting with Opportunistic Routing determines the best path. Packets are authenticated using null keys before transmission. Markov Decision based Adaptive Scheduling decides on the time slot to transmit the authenticated packets.

IV. Multicasting with Opportunistic Routing

In the proposed method we invent a procedure to find the drop ratio for each node in the network. The probability of delivery ratio has to be found to select the active forwarder for carrying out the bundles of packet to next node. The link with low delivery ratio is a weak link and will be discarded from the active path. The following three metrics are used to select the secure path.

- Packet delivery ratio, which is defined as the number of

Golden Julie E. and Harold Robinson Y. are Research Scholar with the Information and Communication Engineering, Anna University, Chennai, India (e-mail: juliegolden18@gmail.com, yhrlcse@gmail.com).

Tamil Selvi S. is Professor & Head of PG Department of ECE, National Engineering College, Kovilpatti, India. (e-mail: tamilgopal2004@yahoo.co.in).

sole multicast bundles which successfully arrive at all the receivers over the total number of bundles that are expected to be received

- Packet delivery efficiency, which is the ratio between the single bundles received by the receivers and the total data transfer generated in the network.

Equations to update the probability of delivery ratio is given as follows

$$P(a,b)=P(a,b)old+(1-P(a,b)old) \times A \qquad (1)$$

$$P(a,b)=P(a,b)old\times Ck \qquad (2)$$

$$P(a,c)=P(a,c)old+(1-P(a,c)old)\times P(a,b)\times P(b,c)\times B \qquad (3)$$

where P(a,b) denotes the delivery predictability of reaching node b from node a and A,B,C are initialization constants chosen from the range[1]. Each node maintains an m*m matrix, with m denoted as the number of nodes in the WSN, where each row i records the delivery predictability of node i to other N-1 nodes. Each node uses (1), (2) and (3) to update its own delivery predictability to other nodes.

- Average end-to-end delay, which is the average of the end-to-end packets delivery latency for each algorithm.

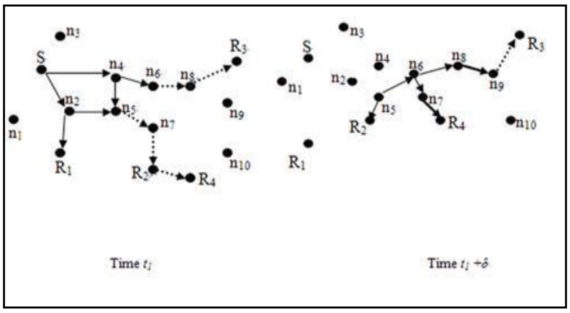

Fig. 2 Probability based OR scheme

Fig. 2 shows path selection based on Opportunistic routing.

V. Packet Authentication

The authentication scheme is inspired by null space originally proposed for defending against pollution attacks. Null key is embedded with transmitted packets. If the receiver identifies the null key then the packet is not a bogus packet [14], [2], [13]. Authentication process consists of the following three phases: Data Pre-processing, Null Key generation and Receiver side authentication.

A. Data Pre Processing

The network coding is applied to a batch of $n - 1$ incoming packets, denoted by $\{Di\}^{n-1}_{i=1}$. For secure transmission, each batch needs a signature packet, denoted as

$$S = M-1\ (hs\ (D_1||\ ...|D_{n-1})) \qquad (4)$$

where M−1 denotes the transmitter's signature using its private key, *hs* is hash function and D represents packet fragment. By using Digital Signature Algorithm (DSA) the packets are signed and verified before sending it to the receiver thus ensuring security [4].

B. Authentication Using Null Keys

The receiver must differentiate between genuine coded packets from bogus ones injected by outsiders. By generating the null key packets, the transmitter optimally sends the null key packets to the receivers to filter out bogus packets.

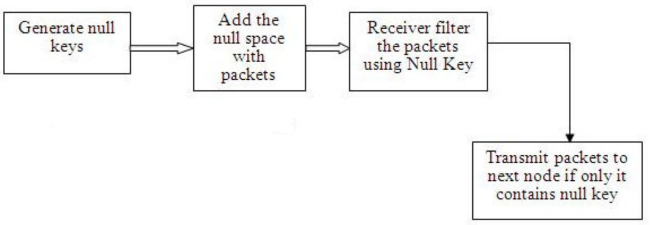
Generate null keys
Add the null space with packets
Receiver filter the packets using Null Key
Transmit packets to next node if only it contains null key

Fig. 3 Null Key Generation

C. Receiver Side Authentication

We implement the following steps for receiver side authentication.

Step 1. Check for valid values of nested hash function from the current batch. If not, verify the signature M−1(*hs*(**v**1−8)) using the transmitter's public key *K*. Otherwise, check if it matches the one in new null key packet. The null packet is dropped if either **v**1−8 does not match or the signature is invalid.

Step 2. Verify the authenticity of the received null key **z***i* using the authentication information along the path. For example, for null key packet *K*1, the receiver checks if

$$\mathbf{v}1-8=hs(hs(hs(hs(\mathbf{z}1)||\mathbf{v}2)||\mathbf{v}3-4)||\mathbf{v}5-8) \qquad (5)$$

Step 3. Using the received null key, check all the received data packets to detect bogus packets, if any.

Step 4. Repeat Step 1 to Step 3 until it reaches the deadline. If the number of coded packets passed the authentication is larger or equal to n, decode the original data packets

$$\{Di\}n,\ i=1. \qquad (6)$$

VI. Markov Decision Process Based Adaptive Scheduling

This section describes how the transmitter adaptively schedules transmissions (data packets and null keys), based on the network state [11], to maximize the network authentication rate. The network dynamics is modelled as a Markov Decision Process (MDP) and at each time slot the transmitter chooses an action from the action set to maximize the accumulative reward at the end of the transmission period. In particular, we specify the network dynamics by a six-tuple (**S**, **A, P**, **r**, *T, γ*), where boldface letters refer to matrix or vector.

Algorithm: Simulation-based Backward Induction Algorithm (SBIA)

```
Input: $S, A, T, \gamma$.
Output: $\pi^* = \{d(s1), d(s2), \ldots, d(sT)\}$
  Initialize: $t = T$, set $V^*(sT) = 0$
for all $s_T \in S$
  for $t := T - 1$ to 1 do
  for each state $s_t \in S$ do
  try all actions $a_t \in A$ for iterations and
   calculate
  $V^*(s_t, a_t) = 1/\Delta\ \Sigma\Delta\ [r(s_t+1|st, a_t) + \gamma V*$
   $(s_t+1)]$
  $V^*(st) = \max_{at\in A\_}\{ V^*(s_t, a_t)\}$
  $d(s_t) = \arg\max_{at\in A}\{\_V^*(s_t, a_t)\}$
  end for
  end for
```

In MDP action set, three actions are identified, namely packet with null key, empty packet and packet with false data. The rewards are given for each node in the transmission path based on action chosen from the action set for successive move without time delay. Based on the rewards at various time slots the optimal policy will be generated to schedule the packets with maximum rewarded time-slots. MDP based Adaptive Scheduling (MAS) implementation of SBIA algorithm is applied to find the time-slot at which slot the packet has to be sent to reward the node based on chosen true action from MDP action set. This analytical function will reduce the time delay on receiver side and also increase the packet delivery ratio on fixed time-slot.

VII. Performance Evaluation

The proposed protocol is compared with CodeOR network Coding scheme. CodeOR uses network coding in opportunistic routing without any scheduling. The metrics considered for comparison are as follows:

Packet Loss Rate (PLR) is a measure of number of packets lost given by

$$\text{PLR} = \text{Packet received/Packets sent by source} \qquad (7)$$

Unsecure links lead to higher loss rate. As seen in Fig. 4 MAS and OR reduce loss rate considerably.

Packet Drop Ratio (PDR) is the relative amount of bundles of packets delivered from the learning history of all nodes. The drop ratio is given by,

$$\text{PDR} = (\text{Packet received by neighbor node/Packets sent by previous node}) * 100 \qquad (8)$$

Fig. 5 shows that the novel approach of routing protocol reduces the packet drop ratio.

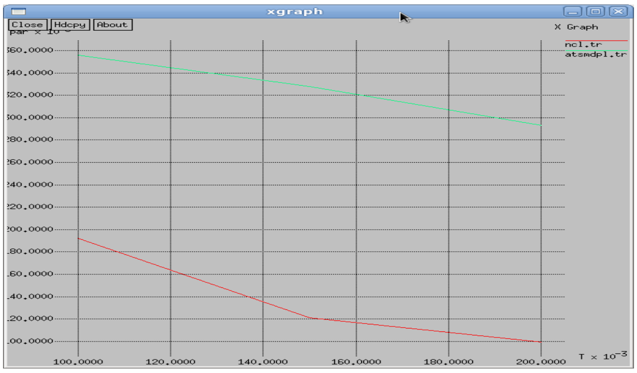

Fig. 4 Comparison Graph for Packet Loss Rate

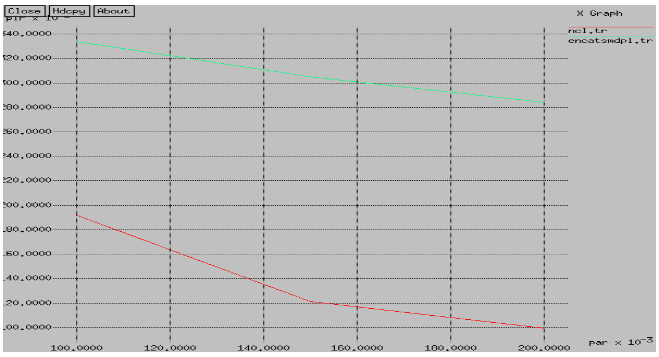

Fig. 5 Comparison graph for PDR

Authenticated Packet Rate (APR) is given by,

$$\text{APR} = \text{No.of packets authenticated/Total no. of packet in channel} \qquad (9)$$

It is calculated as the number of packets authenticated with respect to null key received by the destination. The bogus packets are detected by using this metric. Hence as seen in Fig. 6 DS algorithm provides maximum protection for bundles of packets.

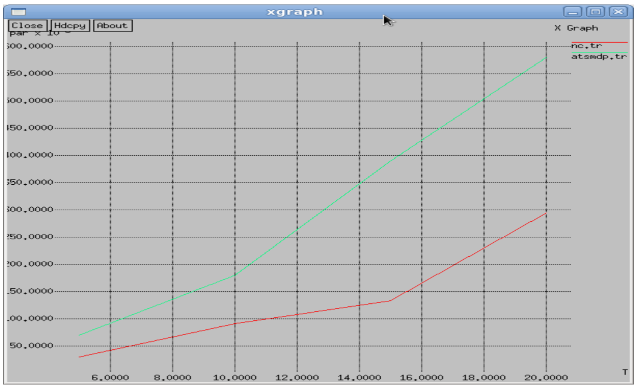

Fig. 6 Comparison graph for APR

Probability of Deliverable Ratio (PPR) is the expected ratio of delivery capability of a node along the transmission path given by,

$$\text{PPR} = 1 - \text{PDR} \qquad (10)$$

Fig. 7 shows the comparison graph for PPR. OR and MAS help in reducing PPR.

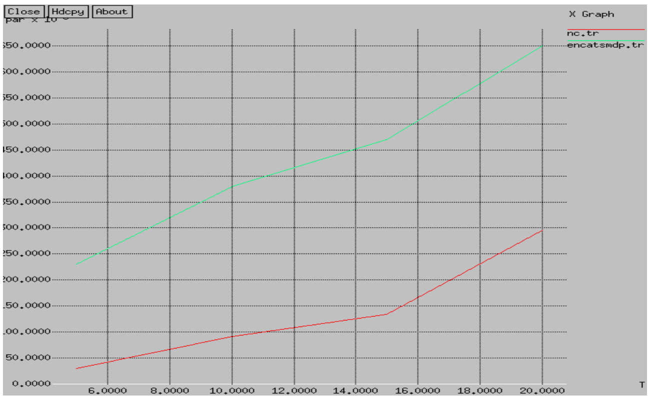

Fig. 7 Comparison graph for PPR

VIII. Conclusion

In this study we have presented a probability-based routing scheme with Adaptive Scheduling to solve the multicast routing problem for WSNs. Simulations based on NS-2 have been carried out to verify the performance of the proposed scheme. To carry out and adopt the optimal transmission method we follow the MDP model and combine Opportunistic routing with Adaptive scheduling. Experimental results confirm that the proposed scheme outperforms Network coded scheme in terms of the packet's delivery-ratio and the standardized routing overhead. It also avoids flooding, pruning and reduces the traffic with very less amount of packet loss in WSNs.

As future work stochastic dynamic programming can be used as a model for sequential decision making when outcomes are uncertain. Energy efficiency in Opportunistic Routing protocol in WSN with advanced MDP scheduling scheme can be considered.

References

[1] A. Kumar, "Comparative performance analysis of versions of TCP in a local network with a lossy link," IEEE/ACM Trans. Netw., vol. 6, pp. 485–498, Aug. 1998.

[2] R. Gennaro and P. Rohatgi, "How to sign digital streams," in Proc. 1997 International Cryptology Conference on Advances in Cryptology.

[3] C. Wong, W. Simon, and S. Lam, "Digital signatures for flows and multicasts," in IEEE/ACM Trans. Networking, 1998.

[4] Y. Wang, P. Le, and B. Srinivasan, "Hybrid group key management scheme for secure wireless multicast," in Proc. 2007 IEEE/ACIS International Conference on Computer and Information, pp. 346–351.

[5] Y. Sun, W. Trappe, and K. Liu, "An efficient key management scheme for secure wireless multicast," in Proc. 2002 IEEE International Conference on Communications.

[6] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: a taxonomy and some efficient constructions," in Proc. 1999 IEEE INFOCOM.

[7] C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," IEEE/ACM Trans. Netw., vol. 8, 2000.

[8] S. Agrawal and D. Boneh, "Homomorphic MACs: MAC-based integrity for network coding," in Applied Cryptography and Network Security, pp. 292–305, 2009.

[9] A. Perrig, R. Canetti, J. Tyagar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," 2000 IEEE Symposium on Security and Privacy.

[10] D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a linear subspace: signature schemes for network coding," in Proc. 2009 PKC, vol. 5443, pp. 68–87.

[11] B. Radunovic, C. Gkantsidis, P. Key, and P. Rodriguez:, "Toward practical opportunistic routing with intrasession network coding for mesh networks," IEEE/ACM Trans. Networking, vol. 18, no. 2, pp. 420–433, 2010.

[12] A. Newell, R. Curtmola, and C. Nita-Rotaru, "Entropy attacks and countermeasures in wireless network coding," in Proc. 2012 ACM Conference on Security and Privacy in Wireless and Mobile Network.

[13] P. Rohatgi, "A compact and fast hybrid signature scheme for multicast packet authentication," in Proc. 1999 ACM Conference on Computer and Communications Security.

[14] T. Ho, M. Medard, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," IEEE Trans. Inf. Theory, vol. 52, no. 10, pp. 4413–4430, 2006.

E.Golden Julie received her B.E degree in Computer Science and Engg in 2005 from Anna University Chennai and ME degree in Computer Science and Engineering in 2008 from Anna University Chennai. Currently she is Pursuing her Ph.D from Anna University Chennai. Presently she is working as assistant professor in Regional centre Anna university, Tirunelveli, India She has published many research papers in various fields. Her research area includes Wireless Sensor Adhoc Networks and Image Processing. She is a member of ISTE

S. Tamil Selvi received her B.E. degree from Madurai Kamaraj University, in 1988, M.E. degree from College of Engineering, Guindy, Anna University, Chennai in 1997 and Ph.D. degree from Manonmaniam Sundaranar University, Tirunelveli in 2009. Presently she is working as Professor in ECE department, National Engineering College, Kovilpatti, India. Her area of interests includes wireless sensor networks and Image Processing, Wireless communication. She has published 24 papers in international journals. She is a fellow of IE (I) and IETE, life member of ISTE and CSI and annual member of IEEE.

Y. Harold Robinson is currently working as an Assistant Professor, dept of CSE in SCAD College of engineering and Technology, Tirunelveli. He finished ME degree in Anna University, chennai. He is Pursuing his Ph.D from Anna University Chennai. His research interests are Wireless networks Mobile Computing, Wireless Sensor Networks. He has published several Research papers in International Journals. He has presented many papers in National and International conferences in Network security, Mobile Computing and Cloud Computing.