Secure Transmission Data Control in Multi Agent System with Attacks and Communication Delays

Duggapu Lakshmi[1], P. Mohana Roopa[2]

Final M.Sc. Student[1], Lecturer[2]
[1, 2] M. Sc Computer Science, Chaitanya Women's PG College, Old Gajuwaka, Visakhapatnam
Andhra Pradesh

Abstract:

Now a days distributed network over multi agent system an important area that have received control community and significant attention from system terms. In multi-agent networks, consensus control as a fundamental distributed control problem has been a hot topic in the past decade due to its wide applications such as sensor networks, traffic control, time synchronization and formation flying. A number of authors have investigated the consensus problems from various perspectives in recent works. Recently, the security and resilience of consensus against malicious attackers in multi-agent systems has attracted attention of researchers. In this paper we are proposed a hybrid bit sequence adhoc vector protocol for finding routing and also provide security of transferring data. By implementing this protocol we can provide two concepts for routing and privacy of data. In the routing process each sender node will find out its neighbour node link is there or not. If there is link between the nodes we can establish connection and continue this process for completion of all nodes in a network. After finding routing we can transfer data from source node to destination node. In this paper we can also calculate delay ration and also provide security of multi agent system over the attacks. By implementing this process we can improve control of multi agent systems and also efficient communication process over the network.

Keywords:

Multi Agent System, Privacy of data, Communication Delay, Security.

I. INTRODUCTION

The study of multi agent system (MAS) has attracted the interests of researchers from various fields for its potential application prospects in distributed computing, sensor networks and multi-robots system. From the viewpoint of automatic control, consensus-oriented flocking and formation control of MAS are widely discussed in previous articles . For all kinds of difficulties appearing in the multiagent system, complex networks involved in synchronization of MAS is among the most significant ones since it is relatively inconvenient to model the exact structure. As a consequence, several entropy measurements have been introduced into the area of multiagent control to describe the property of networks recently In addition, coordination methods are also proposed from entropy view with measurements depicting characteristics of the MAS . Apart from the problems resulting from network, cooperative control of MAS depending on delayed information is also an extensively studied topic due to the inevitabilities of unreliable communication link, bandwidth limitation, packets loss and computing constraint . In this case, in order to guarantee the consensus of the multiagent system, assumptions are usually made about the delays and conditions concerning the control parameters are derived at the same time. Furthermore, for multiagent system with discrete feedbacks, the designed controllers can only rely on sampled states data of agents and the input values are zero-order-hold during sampling instants. As a result, the dynamics of multiagent systems can be presented as discrete ones and the corresponding consensus analyses are also brought out in previous researches. Most of the above mentioned consequences are acquired depending on Lyapunov theory and stochastic matrix theory. For example, in , consensus of the system with communication delays is obtained based on the property of SIA (Stochastic, Indecomposable and Aperiodic) matrix.

In, the leader following consensus problem is solved taking use of Lyapunov-Krasovskii functional. Without any doubt, as two classic methods used in the field of MAS, both Lyapunov theory and stochastic matrix theory have their own advantages. Nevertheless, in order to apply the Lyapunov theory, it is always required that the adjacent matrix of communication graph is symmetric and the results btained can hardly directly extended to the asymmetric situations. On the other hand, to implement results from stochastic matrix, system matrix needs to be nonnegative with row sum value of one. Efforts have been made to overcome these obstacles. In , based on stochastic approximation, ergodicity approach is applied to prove mean square consensus for systems that the existing Lyapunov approaches cannot handle. Through establishing relations between consensus and ergodic backward products, an effective tool to solve consensus problems is proposed. In an auxiliary system is introduced and sophisticated transformations are made to make the consensus analysis more convenient. The requirement that rows of transition matrix are identical plays an important role in the proofs. Actually, it can be viewed as a modification of the unit row sum condition when states of the system, other than error states of the system, are discussed.

Recently, more and more researchers have paid a great deal of attention on distributed coordinated control of networks of dynamic agents within the control community. Especially the consensus problem was discussed widely, which can be attributed to the broad applications of multi-agent systems in many areas, including cooperative control of unmanned air vehicles, formation control of multi-robot, flocking, swarming, distribution sensor fusion, attitude alignment and congestion control in communication networks, etc. In cooperative control of multi-agent system, a critical issue is to design appropriate protocol and algorithms such that all agents can reach a common consensus value. This problem is called consensus problem. In the past decades, some theoretical results have been established in, to name a few. In Vicsek et al. proposed a simple model but interesting discrete-time model of autonomous agents all moving in the plane with the same speed but with different headings. Simulation results provided in show that all agents can eventually move in the same direction without centralized coordination.

II. RELATED WORK

Distributed decision-making for coordination of networks of dynamic agents has attracted several researchers in recent years. This is partly due to broad applications of multi-agent systems in many areas including cooperative control of unmanned air vehicles (UAVs), flocking 1 of birds, schooling for underwater vehicles, distributed sensory networks, attitude alignment of clusters of satellites, and congestion control in communication networks . Agreement problems have a long history in the field of computer science, particularly in automata theory and distributed computation. In many applications involving multiagent/multi-vehicle systems, groups of agents need to agree upon certain quantities of interest. Such quantities might or might not be related to the motion of the individual agents. As a result, it is important to address agreement problems in their general form for networks of dynamic agents with directed information flow under link failure and creation (i.e. variable network topology). Our main contribution in this paper is to define and address consensus problems under a variety of assumptions on the network topology (being fixed or variable), presence or lack of communication time-delays, and boundedness of the inputs of dynamic agents. In each case, we provide convergence analysis and for linear protocols establish direct connections between performance and robustness of a consensus protocol and the properties of graph Laplacian of the information flow in the network.

In the past, a number of researchers have worked in problems that are essentially different forms of agreement problems with differences regarding the types of agent dynamics, the properties of the graphs, and the names of the tasks of interest. In , graph Laplacians are used for the task of formation stabilization for groups of agents with linear dynamics. Their method for formation stabilization has not yet been extended to systems with nonlinear dynamics that are not feedback linearizable. Special cases of this approach are known as leader-follower type architectures and have been widely used by numerous researchers. In graph Laplacians are used in the context of dynamic graph theory. In flocking and heading angle alignment for multiple particles is analysed from the point of view of statistical mechanics and a phase transition phenomenon is observed that occurs the information flow in the network becomes connected. The work in focuses on attitude alignment for undirected graphs in which the agents have simple dynamics motivated by the model used in . It is claimed that the connectivity of the graph on average is sufficient for convergence of the heading angles of the agents. In , the authors addressed convergence of linear and nonlinear protocols for networks with undirected graphs in presence or lack of communication time-delays. Theoretically, analysing consensus on directed graphs is more challenging and is considered in the present paper.

In distributed systems and networks, it is often necessary for some or all of the nodes to calculate some function of certain parameters. For example, sink nodes in sensor networks may be tasked with calculating the average value of all the sensor measurements. A special case of distributed function calculation is the distributed consensus problem, where all nodes in the network calculate the same function. The notion of consensus has recently received extensive attention in the control literature, due to its applicability to topics such as cooperative control of multi-agent systems. In these cases, the approach to consensus is to use a linear iteration, where each node in the network repeatedly updates its value to be a weighted linear combination of its own value and those of its neighbours. These works have revealed that if the network topology satisfies certain conditions, the weights for the linear iteration can be chosen so that all of the nodes asymptotically converge to the same value. Recently, it was shown in that this linear iterative strategy can actually be applied to the more general function calculation problem, allowing any node in the network to calculate an arbitrary function of the node values in a finite number of time-steps.

III.PROPOSED SYSTEM

The main objective of this paper is to design consensus control of multi agent system and which all loyal nodes can resist attackers and resiliently achieve an agreement as time goes to infinity. In this paper we are design an efficient protocol for performing routing and also find attackers in the network. By implementing this protocol we can also calculate packet delivery ration, drop ration and delay ration of each node in the network. Before transferring message from source node to destination node we can identify the destination node is available in the network or not. If the node is available in the network we can find out the node is malicious or not. If the node is not malicious we can transfer data from source node to destination node. Before transferring message from source node to destination node we can find out route. After completion of routing we can convert plain format data into cipher format by using hybrid bit sequence adhoc on distance vector protocol of encryption process. The completion of encryption process the source node will send that information to destination node using the route. The destination node will retrieve the cipher format data and perform the decryption process it will get original plain format data. The implementation procedure of hybrid bit sequence adhoc vector protocol is as follows.

A) Hybrid Bit Sequence Adhoc Vector Protocol:

The implementation procedure of hybrid bit sequence adhoc vector protocol contains three phases. They are

1. Route discovery
2. Monitoring phase
3. Encryption process
4. Decryption process

B) Route Discovery:

In the route discovery source node will broad cost destination node id in the network if the destination id is available it will respond. After responding the destination node not establish connection until the source node will send the data packet. The hybrid bit sequence adhoc vector protocol maintain table to store route information which makes useful to in large networks. In the hybrid bit sequence adhoc vector protocol three kinds of key packets are used path discovery and maintain. In the process route establishment the source node will broad cost request message which contains IP address and last Sequence number of the destination node. This broadcast is received by every neighbour node. Then these neighbour check whether they are actual destination or have a route to the destination. If not then the request message again broad casted. When the request message received by the destination node or the node, which is having a path to destination, it generates a RREP and unicast it back to the source node. On receiving the respond, route discovery process is completed and then the source node starts to send data packets to destination node via established path. Due to mobility or any other reason, if any active link is broken, then request message is Broad casted to all nodes to aware them of route updation. when source node wants to send data to destination its check their routing table if entry is found then it send the data to destination otherwise it starts path discovery procedure and broadcast request packet to his neighbour if their neighbour has path to destination then they send respond to source otherwise they again forward request message to next neighbour. When destination or their intermediate neighbours receive request then it send respond to source node, after receiving respond by source node, it starts sending data to destination.

C) Monitoring phase:

In this phase all the node is work in promiscuous mode means the entire node monitoring his neighbouring node activity, if there is any malicious node left in the network, it does not forward data to next node so his forwarding ratio is decreasing if this ratio is less than threshold values the monitoring node immediately send alert message to source node then source node discard his entry from routing table and send data through neighbour node.

```
Sources send data packets to destination
During transmission every node monitors his neighbour node
If (drop ratio >threshold)
{
Node send alert message to source node
Now source again start route discovery after adding
Malicious node in blacklist

Trap RREQ ()
}
```

After completion of routing process the source node will convert plain format data into cipher format. By performing this process we can implement the encryption process of hybrid bit sequence adhoc vector protocol. The implementation procedure of encryption process is as follows.

D) Encryption Process:

Declaration of variables:

```
            char en[32]= { 0xe2, 0x12, 0xa6, 0x8e,
0x9a, 0xf1, 0x2e, 0x3f,0xe7, 0xca, 0xb1, 0x4e, 0x58,
0x83, 0x3a, 0xe4, 0x13, 0x23, 0x65, 0xae, 0x8e,
0xd4, 0x9d, 0x35, 0x90, 0x3a, 0x63, 0x8e,0x2a,
0x14, 0x54, 0xa2};
            char mm[8];
            char mic_ch;
            char seq_1, seq_2;
            char  mic;
```

```
Void Encrypt (unsigned char * info, int *len)
{
// info: MSG data;
// len: the length of MSG data
seq_1 = 0; seq_2 = 0;
while ( seq_1+seq_2 == 0)
{
seq_1 = rand () % 16; //randomly generating number.
seq_2 = rand () % 16; //randomly generating number.
}
Seq_2 +=16;
for (int i = 0; i< 8; i++)
{
// to produce the encryption table
mm[i] = en [(seq_1+ i) %32] ^ en[(seq_2 + i) %32];
}
mic_ch = 0x5a;
char info_m[ MAXLENGTH];
for (i=0; i < *len; i++)
{
mic_ch = mic_ch ^ info[i];
info_m[i] = info[i] ^ mm[i%8];
mm [i%8] = mm[i%8] ^ en[(seq_1 +8+ i) %32]^
mic_ch;
mic +=info_m[i] ^ en[(seq_1+i)%32] ;
}
info[0] = (seq_1<<4) + seq_2 - 16; // the key bit
sequence
info[1] = mic; // the MIC
for (i=0; i < *len; i++)
{
info[i+2] = info_m[i];
}
*len += 2;
            }
```

After performing the encryption process the source node will send the cipher format data to destination node. The decryption process bit sequence message integrity protocol is as follows.

E) Decryption Process:

The destination node will retrieve the cipher format data and perform the decryption process will get the original message.

```
bool Decrypt(char * info, int *len)
{
 char step_mic;
seq_1 = (info[0]>>4) & 0x0f;
seq_2 = (info[0] & 0x0f) + 16;
step_mic = info[1];
mic = 0;
for (int i = 0; i< 8; i++)
{
mm[i] = en[(seq_1 + i) %32]^ en[(seq_2 + i) %32];
}
mic_ch =0x5a;
for (i=0; i< *len -2 ; i++)
{
mic +=info [i+2] ^ en[(seq_1+i)%32];
info[i] = info[i+2] ^ mm[i%8];
mic_ch = mic_ch ^ info[i];
mm[i%8] = mm[i%8] ^ en[(seq_1 +8+ i) %32]^
mic_ch;
}
if (mic != step_mic) return false;
*len -= 2;
info[*len] = 0;
return true;
}
```

So that by implementing those concepts we can improve efficiency of wireless sensor network and also provide more security of transferring message.

IV.CONCLUSIONS

In this paper we are implementing an efficient protocol for provide secure consensus control of multi agent system in a network. By implementing this protocol we can provide more security of transferred data and also provide efficient route discovery in the network. By perform the route discovery and security of shared data we can implement the hybrid bit sequence adhoc vector protocol. In the implementation of this protocol we can identify the routing from source node to destination node. Before the finding routing the source node will broadcast destination of id in the network. If the destination id is available in the network we can respond and perform the route discovery process. In this process we can also find out malicious node or genuine node and also provide security of transferred message. By implementing this protocol we can provide more security and efficiency of routing discovery.

REFERENCES

[1] Bullo, F.; Cortes, J.; Martinez, S. Distributed Control of Robotic Networks; Applied Mathematics Series; Princeton University Press: Princeton, NJ, USA, 2009.

[2] Aggarwal, C.C. Managing and Mining Sensor Data; Springer: New York, NY, USA, 2013.

[3] Ren, W.; Beard, R.W.; Atkins, E.M. Information consensus in multivehicle cooperative control. IEEE Control Syst. Mag. 2007, 27, 71–82.

[4] Do, K.D. Formation tracking control of unicycle-type mobile robots with limited sensing ranges. IEEE Trans. Control Syst. Technol. 2008, 16, 527–538.

[5] Olfati-Saber, R. Flocking for multi-agent dynamic systems: Algorithms and theory. IEEE Trans. Autom. Control 2006, 51, 401–420.

[6] Tanner, H.G.; Jadbabaie, A.; Pappas, G.J. Flocking in fixed and switching networks. IEEE Trans. Autom. Control 2007, 52, 863–868.

[7] Ren, W.; Sorensen, N. Distributed coordination architecture for multi-robot formation control. Robot. Auton. Syst. 2008, 56, 324–333.

[8] Ren, W.; Beard, R.W.; Atkins, E.M. A survey of consensus problems in multi-agent coordination. In Proceedings of the 2005 American Control Conference, Portland, OR, USA, 8–10 June 2005; pp. 1859–1864.

[9] Ni, W.; Cheng, D. Leader-following consensus of multi-agent systems under fixed and switching topologies. Syst. Control Lett. 2010, 59, 209–217.

[10] Wang, J.; Chen, K.; Ma, Q. Adaptive Leader-Following Consensus of Multi-Agent Systems with Unknown Nonlinear Dynamics. Entropy 2014, 16, 5020–5031.

[11] Anand, K.; Bianconi, G. Entropy measures for networks: Toward an information theory of complex topologies. Phys. Rev. E 2009, 80, doi:10.1103/PhysRevE.80.045102.

[12] Mowshowitz, A.; Dehmer, M. Entropy and the complexity of graphs revisited. Entropy 2012, 14, 559–570.

[13] Van Dyke Parunak, H.; Brueckner, S. Entropy and self-organization in multi-agent systems. In Proceedings of the Fifth International Conference on Autonomous Agents, Montreal, Canada, 28 May–1 June 2001.