International Conference On Emanations in Modern Technology and Engineering (ICEMTE-2017) ISSN: 2321-8169
Volume: 5 Issue: 3 325 - 330

A Study of Consensus Problem in Multiagent System

Supriya More
P. G. Student, Department of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India
Email: moresgm@gmail.com

Sharmila Gaikwad
Assistant Professor, Department of Computer Engineering ,Rajiv Gandhi Institute of Technology, Mumbai, India
Email: sharmila_gaikwad@yahoo.com

Abstract **-** This paper studies the consensus problem in a multi-agent system with random delays governed by a Markov chain. The communication topology is assumed to be directed and fixed. With first order dynamics below the sampled data setting, we first convert the original system into a reduced-order one featuring the error dynamics. Accordingly, the consensus problem is converted into the stabilization of the error dynamic system. Thereafter, based on the theory in stochastic stability for time delay systems, a necessary condition is established in terms of a set of linear matrix inequalities (LMIs). The mean square stability of the error dynamics is shown to guarantee consensus of the multi-agent system. By explicitly incorporating the transition possibility of the random delay into consideration, the conservativeness in control design is reduced. A delay-dependent switching control scheme is studied. Based on the solutions of an algebraic Riccati equation and an algebraic Riccati inequality, a procedure to select the control gains is provided and stability analysis is considered by using Lyapunov's method. A distributed, robust, dynamic, control law is studied such that connectivity preserving rendezvous is achieved regardless of the unknown non-linear dynamics and disturbances.

Index Terms *–Consensus problem, cyber system, strategic attack,attack frequency and attack lengthrate.*

*****

I. INTRODUCTION

Distributed 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 several areas including cooperative control of unmanned air vehicles (UAVs), formation control flocking, distributed sensor networks, attitude alignment of clusters of satellites, and congestion control in communication networks[1].

Recently, results in [2] studied network connectivity preservation when performing locking/rendezvous for multi robot systems. The works in [2] rely on maintaining a connected network among the agents, either for all the time or over sequences of bounded time intervals. The potential field based distributed approaches were developed to address the rendezvous problem while preserving network connectivity.

Our main contribution in this paper is to pose and address consensus problems below a variety of assumptions on the network topology (being fixed or switching), presence or absence of communication time-delays, and directed or undirected network information flow. In each case, provide a convergence analysis. Moreover, establish a connection between algebraic connectivity of the network and the performance of reaching an agreement. Furthermore, demonstrate that the maximum time-delay that can be tolerated by a network of integrators applying a linear consensus protocol is contrariwise proportional to the major eigenvalue of the network topology or the maximum degree of the nodes of the network. This naturally controlled to the realization that there exists a fundamental tradeoff between performance of reaching a consensus and robustness to timedelays.

On the other hand, forcefulness of consensus protocols in networked multi-agent systems to malicious attacks and failures. In [9], detecting and isolating malicious agents in discrete-time linear consensus networks is considered.

In this paper, our analysis relies on several tools from algebraic graph theory [1], matrix theory and control theory. Typically, there are two different attack scenarios in a multi agent system: attack on the dynamic behaviors (or closed-loop dynamics) of the agents and attack on the communications between the agents. Both of attacks can dramatically affect the consensus properties of the whole team. Under the assumption that the network is complete, consensus problem was studied in [14] for multi agent systems with adversaries. Distributed attack detection and identification algorithm via a distributed filter was investigated for cyber-physical systems. An attack on a specific node is identical to node removal on network graphs. In authenticity, it is more general to consider the second attack scenario that a number of edges are attacked [15].The delay could be either constant or time varying, uniform or diverse. A sufficient and necessary condition on the upper bound of the time delay was derived, by analysing the eigenvalues of the transfer function matrix, in which a constraint was imposed on the sum of absolute values of the elements in individually row of the adjacency matrix, and the delays were assumed to be diverse and constant. Both conditions in were delay dependent. Under the discrete-time framework, it was proved that consensus can be reached as long as the time-varying delay has an upper bound and the communication topology has a spanning tree. Such a condition is delay independent.

II. LITERATURE SURVEY

Distributed secure coordinated control of multi agent systems is an interesting and important problem. Multi agent systems, like all large-scale spatially distributed systems, are vulnerable to cyber-attacks due to the growth of network information and communication technologies.

1. The creator Reza Olfati-Saber discuss consensus problems for networks of dynamic agents with fixed and switching topologies provide analytical tools that rely on algebraic graph theory, matrix theory, and control theory. Simulations are provided that demonstrate the effectiveness of theoretical results.
2. The creator Wei Ren introduced that, synchronization of joined second-order linear harmonic oscillators with local interaction. Analyzed convergence conditions over, respectively, directed fixed and switching network topologies by using tools from algebraic graph theory, matrix theory, and non-smooth analysis. It is shown that the coupled harmonic oscillators can be synchronized lower than mild network connectivity conditions. Examples are given to validate the convergence conditions.
3. The creator ZhiFeng studies a robust connectivity preserving rendezvous problem for a leader-following multi-robot system. Only a small group of mobile robots are informed to have access to the leader's information. A distributed, robust, dynamic, control law is proposed such that connectivity conserving rendezvous is achieved regardless of the unknown nonlinear dynamics and disturbances.
4. The creator Yi Dong, Jie Huang introduced that, a leader-following rendezvous problem for a dual integrator multi-agent system where the leader system can generate a class of signals such as ramp signal and sinusoidal signals with arbitrary amplitudes and initial phases.
5. The creator Housheng Su, Michael Z. Q. Chen introduced that, the problem of leader-following consensus of a linear multi-agent system on a switching network. The input of each agent is subject to saturation. Low gain feedback based distributed consensus protocols are developed. It is established that, under the assumptions that each agent is asymptotically null controllable with bounded controls and that the network is connected or together connected.
6. The creator Guoqiang Hu introduced that, the problem of robust consensus tracking for a class of second-order multi-agent dynamic systems with disturbances and un modelled agent dynamics. Contrary to previous approaches, they design continuous distributed consensus protocols to enable global asymptotic consensus tracking. Their focus is on consensus protocol design and constancy analysis which also leads to the derivation of sufficient conditions for consensus tracking.
7. Author Chao Sun, Guoqiang Hu and LihuaXie discussed that, robust consensus tracking problem for a class of high-order multi-agent systems with shown dynamics and unknown disturbances. A continuous robust state response control algorithm is proposed to enable the agents to realise robust consensus tracking of a desired trajectory. By utilizing Lyapunov analysis methods and an invariance-like theorem, sufficient conditions for semi-global asymptotic consensus tracking are recognised. A robust output feedback control algorithm is designed.
8. The creator Shun Chen, Daniel W. C. Ho, discussed distributed adaptive online updating strategies for some parametersbased on local information of the network structure. Then, under the online informing parameters, a distributed adaptive protocol is developed to compensate the fault effects and the uncertainty effects in the leaderless multi-agent system. Based on the local state information of adjacent agents, a distributed updating protocol gain is developed.
9. The creator Heath LeBlanc andXenofonKoutsoukos consider that, a general model for adversaries in Euclidean space and introduce a consensus problem for networked multi-agent systems similar to the Byzantine consensus problem in distributed computing. Adversarial Robust Consensus Protocol (ARC-P), which combines ideas from consensus algorithms that are resilient to Byzantine faults and from linear consensus protocols used for control and coordination of dynamic agents.
10. The makers Iman Shames, Andre M.H. Teixeira, Henrik Sandberg, Karl H. Johansson talked about that, presence of obscure information spectators for systems of interconnected second-arrange direct time invariant frameworks is considered. Two classes of circulated control frameworks of vast handy significance are considered. It is demonstrated that for these frameworks, one can build a bank of obscure information onlookers, and utilize them to identify and seclude blames in the system. The outcome introduces a disseminated execution.
11. The maker Minghui Zhu and Sonia Martínez consider the replay aggressors who perniciously rehash the messages sent from the administrator to the actuator. Propose a variety of the subsiding skyline control law to manage the replay assaults and examinations the subsequent framework execution corruption. A class of focused (resp. agreeable) asset designation issues for flexible arranged control frameworks is likewise explored.
12. The creator Jun Moon and Tamer Bas¸ are introduced that problem for linear time invariant (LTI) systems where the communication loop is subject to a TCP like packet drop network. The problem is formulated within the zero-sum dynamic game framework. The packet drop network is governed by two independent Bernoulli processes that model control and measurement packet losses. Under this constraint, obtain a dynamic output feedback minimax controller.
13. The maker Zhi Feng, Guoqiang Hu and Guanghui Wen are presented two cases. First, under just a class of availability looked after assaults, adequate conditions are determined to accomplish secure agreement following in mean-square. Second, when the multi-specialist frameworks are further subject to a class of network broken assaults, novel adequate conditions are further gotten to guarantee secure accord following with a predefined meeting rate by uprightness of normal abide time exchanging between some steady and precarious subsystems.
14. The maker Zhi Feng talked about a circulated secure accord following control issue for multi specialist

frameworks subject to key digital assaults demonstrated by an irregular Markov handle. A half breed stochastic secure control system is built up for outlining an appropriated secure control law with the end goal that mean square exponential agreement following is accomplished. A network rebuilding instrument is considered and the properties on assault recurrence and assault length rate are explored, individually.An availability reclamation system is accepted to such an extent that after a brief timeframe, the systems can recoup from assaults. The issue is figured from an exchanging point of view and an exchanging arrangement frames an irregular Markov anchor to display vital assaults.

The merits of using Markov chains to characterize delays are as follows.

(1) The random delays in a network exhibit the feature that the occurrence of the current delay depends on the previous delay [14]. The Markov chain model can better characterize the random delay.

(2) By considering the statistical characteristics of the delay in the design, the conservativeness can be reduced, which results in improved system performance. Assume that the delays over all the communication links are the same (uniform) but jumping. By transforming the original system into its reduced order error counterpart, theconsensus problem is converted into stabilization in the mean square sense. A sufficient condition is given through the feasibility of a set of linear matrix inequalities (LMIs).

III. NOTATION AND PRELIMINARIES

For a graph of n nodes denoted by G = (V, E, A), V = {v_1, v_2. . . v_n} is the node set; E ⊆ V × V is the edge set. An edge (v_j, v_i) ∈ E represents the information flow from v_j to v_i . The adjacency matrix A = [a_{ij}] ∈ R^{nxn} , which is nonnegative ($a_{ij} \geq 0$, $\forall_i$, j = 1, 2, . . . , n) in many papers, models the communication topology among the agents. If there is a directed link from agent j to agent i, which means that i receives information from j, then $a_{ij} \neq 0$; otherwise, $a_{ij} = 0$. An undirected graph implies that the communication is bidirectional, i.e., a link from i to j means a link from j to i as well, or else the graph is directed. A path from i to j in a graph is a sequence of distinct vertices starting with i and ending with j such that consecutive vertices are adjacent [13]. The graph Gs' is regarded as a spanning sub graph of G if V(Gs') = V(G) and E(Gs') ⊆ E(G). A spanning tree is a spanning sub graph without cycle. Obviously, in a graph with a spanning tree, there exists at least one node whose information flows to every other node.

The neighbour set of agent i is denoted by N_i , from which i receives information. Thus, N_i = {v_j∈V:(v_j, v_i) ∈ E}. Assume that there is no edge from an agent to itself. In most of the existing work, the adjacency matrix A associated with a graph has the property that $a_{ij} = 0$ and $a_{ij} \geq 0$ for $i \neq j$.

GRAPH THEORY

Variables in lower case refer to scalars, vectors or elements of sets; the distinction will be clear from context. Variables in upper case refer to matrices. When v is a vector, v_i refers to the i^{th} element of that vector, and when v is a set, v_i refers to the i^{th} indexed element of that set. |G| denotes the cardinality of the set G. A_{ij}refers to the element occupying the i^{th} row and j^{th}column of A. The n × n refers to identity matrix.

BASIC DEFINITIONS

A directed graph G consists of a set of vertices, or nodes, denoted V, and a set of arcs A ⊂V , where a = (v, w) ∈ A and v, w ∈ V. The first element of a is denoted tail(a), and the second is denoted the head(a). It is said that a points from v to w. A graph with the property that for any (v, w) ∈ A, the arc (w, v) ∈ A as well is said to be undirected; in undirected graphs the pair of arcs is often modelled as a single edge with no direction associated to it. The in(out)-degree of a vertex v is the number of arcs with v as its head (tail). If every possible arc exists, the graph is said to be complete.

A path on G of length N from v_0 to v_N is an ordered set of distinct vertices {v_0, v_I , . . . , v_N } such that (v_{i-1}, v_i) ∈ A for all i ∈ [1, N]. An N-cycle on G is defined the same as a path except that $v_0 = v_N$, meaning the path rejoins itself. A graph without cycles is said to be acyclic. A graph with the property that the set of all cycle lengths has a common divisor k > 1 is said to be k-periodic.

If a path exists from v_i to v_j , it is said that v_i has access to v_j . A graph with the property that every vertex has access to every other vertex is said to be strongly connected. (A graph consisting of a single vertex with no arcs is also considered strongly connected.) A graph in which disjoint subsets of vertices exists whose elements do not have access to one another is termed disconnected. Note an undirected graph is either strongly connected or disconnected.

The following lemma provides some spectral properties of the Laplacian matrix L.

*Lemma 1 :*Denote the Laplacian matrix $L = [l_{ij}]$ where

$$l_{ij} = \begin{cases} \sum_{k=1,k\neq i}^{n} a_{ik} \ , i = j \\ -a_{ij} \ ; i \neq j \end{cases} \quad (1)$$

Then, the following statements are true:

(i) Zero is a simple eigenvalue of *L*, and 1*n* is the corresponding eigenvector, that is *L*1*n* = 0.

(ii) If *G* has a directed spanning tree, then the eigenvalue 0 is algebraically simple for its Laplacian matrix, and all the other eigenvalues have positive real parts.

Lemma 2 :

Suppose that matrix A = [a_{ij}]∈$R^{(nxn)}$has $a_{ij} \leq 0$ for all $i \neq j$, i, j ∈ {1, · · · , n}. Then, the following statements are equivalent:

1) A is a nonsingular M-matrix.

2) There exists a positive definite diagonal matrix

$$\Theta = \text{diag}\{ \theta{-}11 , \theta{-}12 , \cdots , \theta{-}1n\}$$

such thatQ = ATΘ + ΘA >0.(2)

3) All the eigenvalues of A have positive real parts.

IV. PROBLEM FORMULATION

Consider a class of stochastic linear multi-agent systems with the i^{th} agent described as

$$dx_i(t) = [Ax_i(t) + Bu_i(t)]\, dt + f(x_i(t), t)dw_i(t), \quad (3)$$

Where $x_i(t) \in R^l$is the system state, $u_i(t) \in R^l$is the control input, i = 1, 2, · · · , n,, $w_i(t)$ denotes a one dimensional Brownian motion satisfying
E $\{dw_i(t)\}$ = 0and E$\{dw_i^2(t)\}$= dt, f $(x_i(t),t)dw(t) \epsilon R^l]\}$(4)
Is a continuously differentiable function, and A andB are constant matrices with compatible dimensions.
For simplification,
Let

$$f(x_i(t), t) = (f_1(x_i(t), t), f_2(x_i(t), t), . . , f_l(x_i(t), t))^T . \quad (5)$$

The objective is to design a distributed protocol $u_i(t)$ for system such that all the followers track the leader under two types of attacks. The leader for consensus tracking, labeled as i = 0, is generated as

$$dx_0(t) = Ax_0(t)dt + f(x_0(t), t)dw_0(t), \quad (6)$$

Where $x_0(t) \in R^l$is the state of the leader. Consider the information exchange between the n agents and the leader. A diagonal matrix $\Delta = diag\{\Delta_1, \Delta_2, \cdots, \Delta_n\}$ is used to represent the access of agents to the desired trajectory. If Δ_i, i ∈ {1, 2, · · · , n} is equal to 1, then the i^{th} agent has access to the desired trajectory, and 0 otherwise.
A matrix H as H = L+Δ, which is named as the information-exchange matrix.

*Assumption 1:*The pair (A,B) is stabilizable.
*Assumption 2:*There exists a constant ρ >0, such that
$\|f(y, t) - f(z, t)\| \leq \rho \| y - z \|; \forall y, z \in R^l, t \geq 0.$
Definition 1:
(*Connectivity-maintained attacks*) Under connectivity-maintained attacks, the original network topology with a directed spanning tree still possesses a directed spanning tree, even though the topology changes due to link failures or creation of new links.

Definition 2:
(*Connectivity-broken attacks*) Under connectivity broken attacks, the original network topology with a directed spanning tree become disconnected due to attack-caused link failures.

V.MEAN-SQUARE EXPONENTIAL CONSENSUS TRACKING UNDER STRATEGIC ATTACKS

A distributed secure consensus tracking control problem is studied for multi agent systems (4) under strategic attacks. In the context of multi agent systems, the initial connectivity graph of the agents often meets some connection conditions [14]. Thus, motivated by this observation, assume that the initial graph without being attacked by any strategic attacks contains a directed spanning tree with the leader being the root. However, strategic attacks satisfying a random Markov jump process may make the networks paralyzed as the graph communication connectivity is broken, which results in the loss of secure consensus tracking performance for the entire multi agent systems.

1) Cyber System: The state of the cyber system is described by θ(t). The evolution of θ(t) depends on the attacker's action a and the cyber defense action d, which are also functions of time. For a given pair (a, d), θ(t) is modeled as a right continuous, time-homogeneous, ergodic, and random Markov process. S = {1, 2. . . s} is the finite state space corresponding to all possible topologies under attacks. Let the infinitesimal generator of Markov process be $\Upsilon = (\gamma_{pq})$, which is given by
$P_{pq}(t)$=Prob[r(t+h)=q | r(t)=p]

$$= \begin{cases} \gamma pqh + o(h), p \neq q \\ 1 + \gamma pph + o(h), p = q \end{cases} \quad (7)$$

Where for the switching signalr(t), $\gamma_{pq} > 0$ is the transition rate from state p to state q if p≠q while $\gamma_{pp} = -\sum_{q=1,p\neq q} \gamma_{pq}$ and o(h) denotes an infinitesimal of higher order than h.Υ is transition rate matrix.
Compared with the existing results that an attack on a node (or a fraction of nodes) is identical to node removal (complete loss of its functionalities) on the corresponding network, in this paper consider attacks on the communication links E but not on the nodes V: That is, an attack removes or adds the edges instead of nodes in the network. The considered attacks on the edges may cause the loss of secure consensus tracking performance.

*2) Cyber Strategy:*Denote by $a \in A$ a cyber-attack chosen by the attacker from its attack space $A := \{a1, a2, . . . , am\}$ composed of all *m* possible actions. $d \in D$ is the cyber defense mechanism employed by the network administrator, which includes possible defense actions from $D := \{d1, d2, . . . , dn\}$. Thus, one can consider the following mixed strategies of the defender and the attacker:

$$F(k) = [f_p]_{p=1} \in F_k, g(k) = [g_q(k)] \in G_k \quad (8)$$

$$F(K) := \{F(k) \in [0,1]: \sum_{p=1}^{n} F_p(k) = 1\} \quad (9)$$

$$G(K) := \{g(k) \in [0,1]: \sum_{q=1}^{m} g_p(k) = 1\} \quad (10)$$

Where *k* denotes the time scale on which cyber events occur, $f_p(k)$ and $g_q(k)$are the probabilities of choosing $dp \in D$ and $a_q \in A$, respectively, and *F(k)* and *G(k)* are two sets of admissible strategies provided for the defender and the attacker. Therefore, the transition law of the cyber system state *θ(k)* at time *k* depends on the actions of the attacker as well as thedefense mechanism employed by the network administrator.
More precisely, the rate matrix satisfies

$$\text{Prob}\{\theta(k+\Delta)=q \mid \theta(k)=p\} = \begin{cases} \gamma pq(f(k), g(k), q \neq p \\ \gamma pq(f(k), g(k), q = p \end{cases} \quad (11)$$

Where Δ >0 is on the same scale as *k*, γpq(f (k), g(k))are the average transition rates in terms of the transition rates$\tilde{\gamma} pq(k)$ = $\tilde{\gamma}$pq(aq(k), dp(k)), p, q ∈S, defined by

$$\gamma_{pq}(f(k), g(k) = \sum_{p=1}^{n} \sum_{q=1}^{m} f_p(k) g_q(k) \gamma_{pq}(k) \quad (12)$$

*Remark 1:*Definition 1 implies that the topology with a directed spanning tree provides the possibility to guarantee consensus tracking security of the overall multi-agent systems, while in Definition 2, the topology under connectivity-broken attacks without any directed spanning trees will bring negative effect and might totally destroy the secure consensus tracking performance.
Remark 2:
It is reasonable to model the aforementioned two types of connectivity-maintained/broken attacks from a switching perspective.

VI. ATTACKER AND DEFENDER STRATEGIES

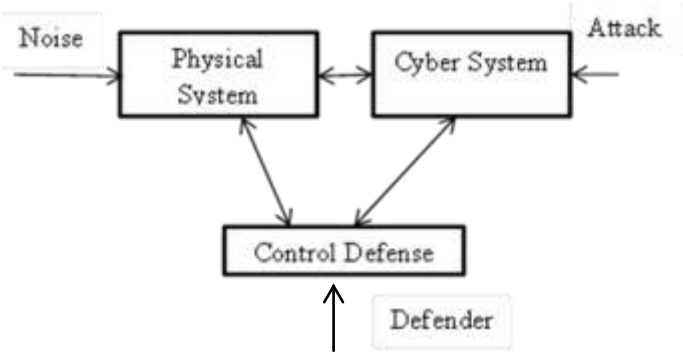

Fig 1: Framework of the attacker and defender strategies in a multi agent system

In a networked multi-agent system, the attacker aims to remove the connection edges in a network such that the possible network topologies do not have a directed spanning tree. The defender aims to reconstruct a number of edges in the network based on a recovery mechanism such that the network topology still has a spanning tree [13]. A resilient distributed algorithm is then developed such that the network would not loss the secure consensus tracking performance. The framework of the attacker and defender strategies is shown in Figure 1. The interactions between the cyber and physical systems are captured by their dynamics, where the physical state and the cyber stateare controlled by the defense mechanism used by the network defender as well as the attacker's action.

Remark 3: Existing Attack Strategies as Subcases:
i) Stealth attacks defined in [15] correspond to output attacks compatible with the measurements equation;
ii) Replay attacks defined in [15] are state and output attacks which affect the system dynamics and reset the measurements;
iii) Covert attacks defined in are closed-loop replay attacks, where the output attack is chosen to cancel out the effect on measurements of the state attack;
iv) (Dynamic) false-data injection attacks defined in are output attacks rendering an unstable mode (if any) of the system unobservable [15].

A. Time-Varying Markovian Graph

Based on descriptions of attack model in [14], let $G_{r(t)} = \{V, \varepsilon_{r(t)}, A_{r(t)}\}$ represent a directed time-varying graph of order N with the set of nodes V, $\varepsilon_{r(t)}$ is the set of edges and $A_{r(t)} = [a_{ij}^{r(t)}] \in R^{(NXN)}$ denotes the adjacency matrix of $G_{r(t)}$, where $a_{ij}^{r(t)} > 0$ if and only if (j, i) $\in \varepsilon_{r(t)}$ else $a_{ij}^{r(t)} = 0$. An edge of $G_{r(t)}$ is an ordered pair (i, j) $\in \varepsilon^{r(t)}$ if agent j can be directly supplied with information from agent i. The set of neighbors of node vi is denoted by $N_{r(t)} = \{v_i \in V, (v_j, v_i) \in \varepsilon_{r(t)}, j = i\}$ [1]. Graph $G_{r(t)}$ contains a directed spanning tree if there is a node which can reach all the other nodes through a directed path. The Laplacian matrix of a graph $G_{r(t)}$ is defined as $L_r(t) = D_{r(t)} - A_{r(t)} \in R^{(NXN)}$, Where,

$$D_{r(t)} = \text{diag}\{d_1^{r(t)}, d_2^{r(t)}, \ldots, d_N^{r(t))}\} \text{ with}$$
$$d_i^{r(t)} = \sum_{j=1}^{n} a_{ij}^{r(t)} \quad (13)$$

Thus, an information-exchange matrix for consensus tracking is written as,

$$H_{r(t)} = L_{r(t)} + B_{r(t)}, \text{ where } B_r(t) = \text{diag}\{b_1^{r(t)}, b_2^{r(t)}, \ldots, b_N^{r(t)}\} \quad (14)$$

represents the access of followers to the leader under attacks. If $b_i^{r(t)} = 1$, the i^{th}agent accesses to leader, and $b_i^{r(t)} = 0$, otherwise.

B. Connectivity Restoration Mechanism

In order to achieve secure consensus tracking for system under strategic attacks, the following assumption introduces a connectivity recovery mechanism [14].
Assumption 3:$G_{r(t)}$ can be recovered into connectivity maintained topologies after a connectivity restoration mechanism (i.e., the sensing and communication devices are able to recover through some backup or repairing efforts).
Remark 4: Although the initial graph without being attacked can provide the possibility of consensus tracking for system, each paralyzed topology $G_{r(t)}$ under strategic attacks might totally destroy the secure consensus performance of the whole multi agent systems. Thus, Assumption 3 implies that the secure consensus tracking problem can be solved if there exists a connectivity restoration mechanism through internal recovery/tolerance capacities of the system or repairing efforts, even though it may take a short period of time [14].

C. Attack Frequency and Attack Length Rate

Definition 3 (Attack Frequency):
Based on [14], for any $T2 > T1 \geq t_0$, let N_f (T1, T2) denote the number of attacks taking place over [T1, T2]. Thus, F_f (T1, T2) = N_f(T1, T2)/(T2 − T1) is defined as the attack frequency over [T1, T2] for all $T2 > T1 \geq t_0$.

Definition 4 (Attack Length Rate):
Based on [14] , for any $t > 0$, denote $T_a(t_0, t)$ as the total time interval for multi agent systems under attacks during [t0, t). Thus, $T_a(t_0, t)/(t - t_0)$ is defined as the attack length rate over $[t_0, t]$.

VII. FUTURE SCOPES

By In the end, the mobile-agent research community should strive to contribute by improving our understanding of the value of mobility, by distilling our ideas into a core set of concepts, by encouraging the construction of those concepts as a set of compostable software components, by educating those outside our community about the value of mobility, and by demonstrating its value through the its use in real applications and middleware.

The architecture projected in general and the agents in particular, could easily detect application-layer intrusions. Thus, further study will focus on the improvement in the system by covering any potential vulnerability. For this to happen, require needs all the packets involved in the intrusions and gathered by the agents.

VIII. CONCLUSION

A distributed secure consensus tracking problem is studied for both continuous-time and discrete-time linear multi agent systems under strategic attacks in cyber system whose dynamics are captured by a random Markov process. Author formulates this problem from the perspective of a switched system with two-level switching sequences. Under the hybrid stochastic secure control framework, a distributed resilient control law is studied to achieve exponential consensus tracking in mean square sense, provided that two conditions on the attack frequency and attack length rate are satisfied.

REFERENCES

[1] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," IEEE Trans. Autom. Control, vol. 49, no. 9, pp. 1520–1533, Sep. 2004.

[2] W. Ren, "Synchronization of coupled harmonic oscillators with local interaction," Automatica, vol. 44, no. 12, pp. 3195–3200, 2008.

[3] Z. Feng, C. Sun, and G. Hu, "Robust connectivity preserving rendezvous of multi-robot systems under unknown dynamics and disturbances," IEEE Trans. Control Netw. Syst., to be published, doi: 10.1109/TCNS.2016.2545869.

[4] Y. Dong and J. Huang, "A leader-following rendezvous problem ofdouble integrator multi-agent systems," Automatica, vol. 49, no. 5, pp. 1386–1391, 2013.

[5] H. Su, M. Z. Q. Chen, J. Lam, and Z. Lin, "Semi-global leader-following consensus of linear multi-agent systems with input saturation via low gain feedback," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 60, no. 7, pp. 1481–1489, Jul. 2013.

[6] G. Hu, "Robust consensus tracking of a class of second-order multiagent dynamic systems," Syst. Control Lett., vol. 61, no. 1, pp. 134–142,2012.

[7] G. Wen, G. Hu, W. Yu, and G. Chen, "Distributed H∞ consensus ofhigher-order multiagent systems with switching topologies," IEEE Trans.Circuits Syst. II, Exp. Briefs, vol. 61, no. 5, pp. 359–363, May 2014.

[8] S. Chen, D. W. C. Ho, L. Li, and M. Liu, "Fault-tolerant consensus of multi-agent system with distributed adaptive protocol," IEEE Trans. Cybern., vol. 44, no. 10, pp. 2142–2155, Oct. 2015.

[9] H. J. LeBlanc and X. D. Koutsoukos, "Consensus in network de multi-agent systems with adversaries," in Proc. 14th Int. Conf. HybridSyst. Comput. Control, Chicago, IL, USA, Apr. 2011, pp. 281–290.

[10] I. Shames, A. M. H. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems,"Automatica, vol. 47, no. 12, pp. 2757–2764, 2011.

[11] M. Zhu and S. Martínez, "On the performance analysis of resilientnetworked control systems under replay attacks," IEEE Trans. Autom. Control, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[12] J. Moon and T. Basar, "Control over lousy networks: A dynamic gameapproach," in Proc. Amer. Control Conf., Portland, OR, USA, Jun. 2014,pp. 5367–5372.

[13] Z. Feng, G. Hu, and G. Wen, "Distributed consensus tracking formulti-agent systems under two types of attacks," Int. J. Robust. Nonlin. Control, vol. 26, no. 5, pp. 896–914, 2015.

[14] ZhiFeng "Distributed Secure Coordinated Control for Multi agent Systems under Strategic Attack .2168-2267_c2016IEEE.

[15] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identificationin cyber-physical systems," IEEE Trans. Autom. Control, vol. 58,no. 11, pp. 2715–2729, Nov. 2013.